ＩＮＦＯＮＥＴ－ＶＰ１００

ＶＰＮボックス 取扱説明書

古河電気工業株式会社

ご注意

① この装置の耐用年数は6年です．それ以降の使用は弊社にご相談ください．

② この装置の修理可能期間は，製造終了後6年間とさせていただきます．
本マニュアルには，「外国為替及び外国貿易管理法」に定める戦略物資関連技術が含まれています. 従って, 本マニュアルを輸出する場合には, 同法に基づく許可が必要とされます. なお, 本マニュアルを廃棄する場合は，完全に粉砕して下さい．

この装置は，情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスＡ情報技術装置です．この装置を家庭環境で使用すると電波妨害を引き起こすことがあります．この場合には使用者が適切な対策を講ずるよう要求されることがあります．

安全のために

⚠ 警告	下記の注意事項を守らないと火災・感電により死亡や、大けがの原因となります。

設置について

本装置の分解・解体・改造・再生を行わないでください．また，本装置の上には絶対に重いものをのせないでください．

ケーブルについて

本装置に接続してあるケーブル類の上には絶対に重いものをのせたり，折り曲げたりしないでください．

使用上の注意

電源ケーブルがACコンセントに接続されているときには，濡れた手で本装置に触れないでください．感電の原因となります．

本装置の電源は，AC100V（50/60Hz）を使用してください．
異なる電圧で使用すると，感電，発煙，火災の原因となります．

本装置内部には，水などの液体を入れないでください．
感電の原因となります．

雷が鳴り出したら，ケーブルや電源ケーブルに触れないでください．
感電の原因となります．

注意 下記の注意事項を守らないと火災・感電により死亡や、大けがの原因となります。

設置について

本装置は，屋内に設置してください.
故障の原因となります.

極端な高温，あるいは低温状態や温度変化の激しい場所で使用しないでください.
故障の原因となります.

直射日光の当たる場所や発熱機器（ストーブ，コンロなど）のそばで使用しないでください．故障の原因となります.

水や油などの液体がかかる場所，湯気がかかる場所，湿気やほこりの多い場所で使用しないでください．火災・感電・故障の原因となります.

塩害地域では使用しないでください.
故障の原因となります.

衝撃や振動の加わる場所で使用しないでください.
故障の原因となります.

薬品の噴囲気中や薬品にふれる場所で使用しないでください.
故障の原因となります.

モータなど，強い磁界を発生する装置のそばで使用しないでください.
故障の原因となります.

ラジオやテレビジョン受信機等のそばで使用しないでください.
ラジオやテレビジョン受信機等に雑音が入る場合があります.

本装置は側面に内部の熱を逃がすための通気孔が設けてあるので，装置の側面に物を置いたりして，通気孔をふさがないでください.
通気孔をふさぐと，内部の温度が上昇して，故障の原因となります.

本装置をならべて使用する場合，側面に3cm以上の間隔をあけてください.
故障の原因となります.

国内のみで使用してください.
本装置は国内仕様になっていますので，海外ではご使用になれません.

ケーブル

本装置のケーブル類を抜き差しする場合には，先に装置の電源ケーブルを抜いてください．

本装置のケーブル類は，足などを引っかけないように整理してください．
ケーブル類に足などを引っかけると，危険です．
また，本装置の使用中に電源ケーブルが抜けると，重要なデータが失われることもあります．

電源

安全のために，電源（AC100V）コンセントには，必ずアースを取ってください．
アースを接続しないと，感電の原因となります．

本装置の電源ケーブルは，タコ足配線にしないでください．
コンセントが過熱し，火災の原因となることがあります．

使用上のご注意

内部に液体や金属類など異物が入った状態で使用しないでください．
故障の原因となります．

本装置を移動するときは，必ず電源ケーブルを抜いてください．
故障の原因となります．

本装置のお手入れ

汚れを落とす場合は電源ケーブルを抜いてから，やわらかい布によるからぶきか，水または中性の洗剤を含ませて固くしぼった布で軽く拭いてください．
水や中性洗剤は，絶対に本体に直接かけないでください．

ベンジンやシンナーなど（揮発性のもの）は使用しないでください．
本装置の外装を傷めたり，故障の原因となったりします．

殺虫剤などをかけないでください．
故障の原因となります．

本装置の廃棄方法

本装置を廃棄するときは，地方自治体の条例にしたがって処理をしてください．詳細は，各地方自治体に問い合わせてください．

著作権および商標について

本装置のファームウェアには以下の著作権が含まれています.

GateD, Release 3.Copyright (c) 1990, 1991, 1992 by Cornell University. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Cornell University and its collaborators. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

GateDaemon Project
Information Technologies/Network Resources
143 Caldwell Hall
Cornell University
Ithaca, NY 14853-2602

GateD is maintained and developed by Cornell University and its collaborators.

商標

Contains SSH IPSEC technology (pat.pending).
SSH is a registered trademark of SSH Communications Security Ltd.
(http://www.ssh.fi)

はじめに

このたびは，INFONET-VP100 VPN ボックスをお買い上げいただき，まことにありがとうございます．本取扱説明書は，INFONET-VP100 VPN ボックスの基本的な取扱いについて説明しています．ご使用の際には，本取扱説明書をお読みになり，正しくご使用くださるようにお願い申し上げます．また，本装置をご使用になる間は，本取扱説明書を大切に保管してください．

尚，本製品および本取扱説明書を正しくお使いいただく上で以下の前提知識を必要とします．

前提知識

－ LAN（Local Area Network）IEEE802.3/Ethernet 規格，または同程度の知識を有していること．

－ TCP/IP（Transmission Control Protocol / Internet Protocol）の知識を有していること．

－ SNMP（Simple Network Management Protocol）およびMIB（Management InformationBase）のネットワーク管理についての知識を有していること．

－ コンピュータの一般知識を有し，キーボード操作ができること．

まず，梱包物をご確認ください．

梱包物

－ INFONET-VP100 VPN ボックス　１台
－ 取扱説明書（本書）　１部
－ コマンドリファレンス　１部
－ ユーザ登録カード　１枚

万一不備な点がございましたら，恐れ入りますがお買い求めの販売店までお申し付けください．

保証について

弊社ではユーザ登録をお願いしております．お手数ですが「ユーザ登録カード」にご記入の上，弊社までご返送くださいますようお願いいたします．また，保証書は１年間大切に保管してください．

弊社ではお買い上げいただきました製品に対し，お買い上げ後１年間の無償保証を行っております．正常なご使用状態のもとで，保証期間内に万一故障が発生いたしました時は，下記の弊社サポート窓口にお問い合わせください．

その場合，保証書に従い故障の修理をさせていただきます．

サポート窓口

古河電気工業株式会社
ネットワーク事業部　INFONET サポートセンター
〒153-0043　東京都目黒区東山 1-1-2 東山ビル 2F
TEL:03-5721-5169（ダイヤルイン）　FAX:03-3760-2167
コール受付時間：平日（月～金）9 時～12 時，13 時～17 時
（祝祭日，年末年始（12/29～1/5），弊社休日を除く）

本書の構成と内容

本取扱説明書は，本装置の設置・設定・運用等に関して記述されています．本書は，以下のように構成されています．

１章：装置の導入

装置の外観や取扱い上の注意事項について説明しています．
装置を設置する前にお読みください．

２章：機能概要

装置の機能について説明しています．

３章：設定を始める前に

装置の設定を行うために，コンソールの接続方法を説明しています．

４章：LANについて

装置を LAN に接続する際の注意事項を紹介しています．

５章：IPルーティングに関する設定

IP ルーティングを使用するための設定を説明しています．

６章：IPSEC機能に関する設定

IPsec を使用するための設定を説明しています．

７章：NAT（アドレス変換）設定

NAT（アドレス変換）を使用するための設定を説明しています．

８章：DHCPサーバ機能

DHCP サーバ機能を使用するための設定を説明しています．

９章：SYSLOG機能

SYSLOG 機能について説明しています．

１０章：SNMPエージェント機能

SNMP エージェント機能について説明しています．

１１章：インフォメーション

各種情報表示について説明しています．

１２章：オペレーション

本装置で行える操作について説明しています．

本書で使用される用語について

用語の説明

(1) 構成定義情報

装置の運用に関する設定情報を示します.

(2) フィルタリング

本取扱説明書でフィルタリングという表現があった場合は，中継するデータを限定する場合と，遮断するデータを限定する場合の 2 通りがあります.

(3) IP アドレス

本取扱説明書で使用している IP アドレスは，ローカルなネットワークで使用されるアドレスとして推奨されているものです（RFC(Request For Comments)1597）．したがって，本取扱説明書中のアドレスを使用して，外部のネットワークと接続することはできませんので，ご注意下さい．本取扱説明書の IP アドレスは，以下の範囲内のものです.

10.0.0.0 ～ 10.255.255.255
172.16.0.0 ～ 172.31.255.255
192.168.0.0 ～ 192.168.255.255

本取扱説明書では，xxx.xxx.xxx.xxx の形式の表記方法を「IP アドレス形式」と記述しています.

(4) MAC アドレス

本取扱説明書で使用している MAC アドレスは，実際には存在しない MAC アドレスを使用しています．したがって，本取扱説明書と同じ MAC アドレスは，装置に入力できません．本取扱説明書中の MAC アドレスの例としては，以下のものがあります.

xx:xx:xx:xx:xx:xx
XX:XX:XX:XX:XX:XX
YY:YY:YY:YY:YY:YY
ZZ:ZZ:ZZ:ZZ:ZZ:ZZ

本取扱説明書では，xx:xx:xx:xx:xx:xx の形式の表記方法を「MAC アドレス形式」と記述しています.

(5) 画面例

本取扱説明書で表記している画面例は，使用する機能の違いにより，実際の画面と異なる場合があります.

注釈マークの説明

本取扱説明書で使用している記号の意味は以下のとおりです.

お知らせ

装置の設定，運用に関する参照先や補足の説明，特に意識すべき注意点を示します.

設定情報一覧表中の，◎は設定が必須な項目，○は使用するためには設定（確認）が必要な項目，×は導入時の設定で問題ない項目を示しています.

1　装置の導入

この章では，本装置の各部の名称と機能，ケーブルの接続方法，取扱い上の注意，公衆回線網の加入契約条件等装置の導入に関して説明します．

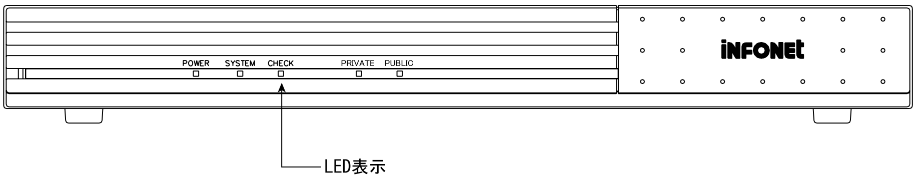
装置を使用する前に必ずお読みください．この章の内容を以下にまとめます．

- 各部の名称と機能
- 電源の投入／遮断
- 各ケーブルの取扱い
- LED 表示

１．１ 各部の名称と機能

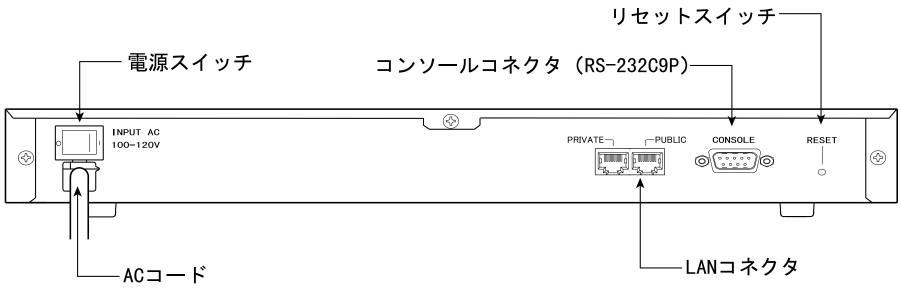
以下に本装置の各部の名称を示し，その機能を説明します.

装置前面



－　LED 表示

LED 表示によって現在の運用状態を示します.



装置後面

－　電源スイッチ

電源の ON／OFF を行うスイッチです.

－　電源ケーブル

３極ストレート AC100V コンセントに接続するためのケーブルです.

お知らせ

－　10BASE-T ポート

本装置と端末を接続するツイストペアケーブル（モジュラケーブル）を接続するポートです．別売りのツイストペアケーブル（モジュラケーブル）を接続します．

－　コンソールポート

装置の運用状態の表示，コマンドの操作，構成定義情報の表示，設定および変更を行うために RS-232C インタフェースを持つ端末を接続するためのポートです．

－　リセットスイッチ

装置のリセットを行うスイッチです．

装置底面

－　VCCI・EC 版数銘板

VCCI（情報処理装置等電波障害自主規制協議会）基準に基づく注意書きを示します．

－　製造銘板

装置名称，シリアル番号，製造年月，装置版数を示します．

－　PL ラベル

装置運用上の注意事項を示します．

1.2 電源の投入／遮断

電源の投入／遮断は電源スイッチにより行います.

- 電源をONにする場合，電源スイッチを「|」側に押します.
- 電源をOFFにする場合，電源スイッチを「○」側に押します.

電源投入後は，前面のPOWERランプが点灯します.

1.3 各種ケーブルの取扱い

本装置を導入するためには，各種ケーブルを接続する必要があります．以下のケーブルの取扱い方法を説明します．

－　コンソールケーブル（別売）

－　10BASE-T ケーブル（別売）

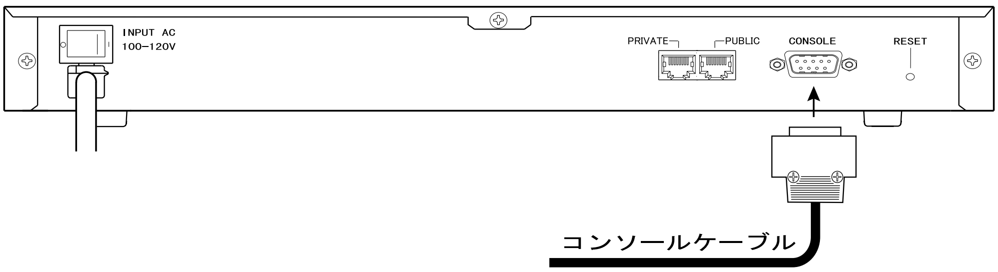
お知らせ

各ケーブルの接続は装置の電源スイッチが OFF（「○」側に押されている状態）であることを確認してから行ってください．

コンソール

コンソールの接続は以下の方法で行ってください．

（1）コンソールポートにコンソールケーブル（クロスケーブル）を接続します．
（2）コンソールケーブルコネクタのスクリューロックを回し，コネクタを固定します．
（3）お手持ちのコンソールに同様にしてコンソールケーブルを接続します．
（4）コンソール使用終了後はコンソールケーブルを取り外してください．



お知らせ

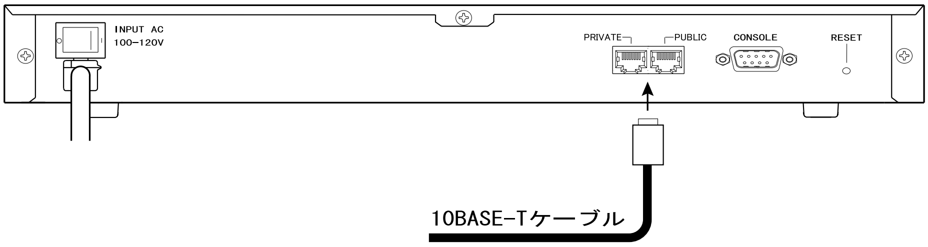
コンソールには，RS-232C 規格インタフェースを持った機器をご使用ください．コンソールポートに接続するコンソールの通信機能は，「付録Ａ　装置の仕様」を参照してください．

お知らせ

本取扱説明書では，コンソールポートに接続したコンソールを「ローカルコンソール」と表現する場合もあります．

10BASE-Tケーブル

10BASE-T ポートにツイストペアケーブルのモジュラコネクタを「カチン」と音がするまで差し込んでください.



1.4 LED 表示

本装置の運用状態は，装置前面の LED 表示ランプによって示されます.
LED 表示ランプのそれぞれの動作と意味を以下に示します.

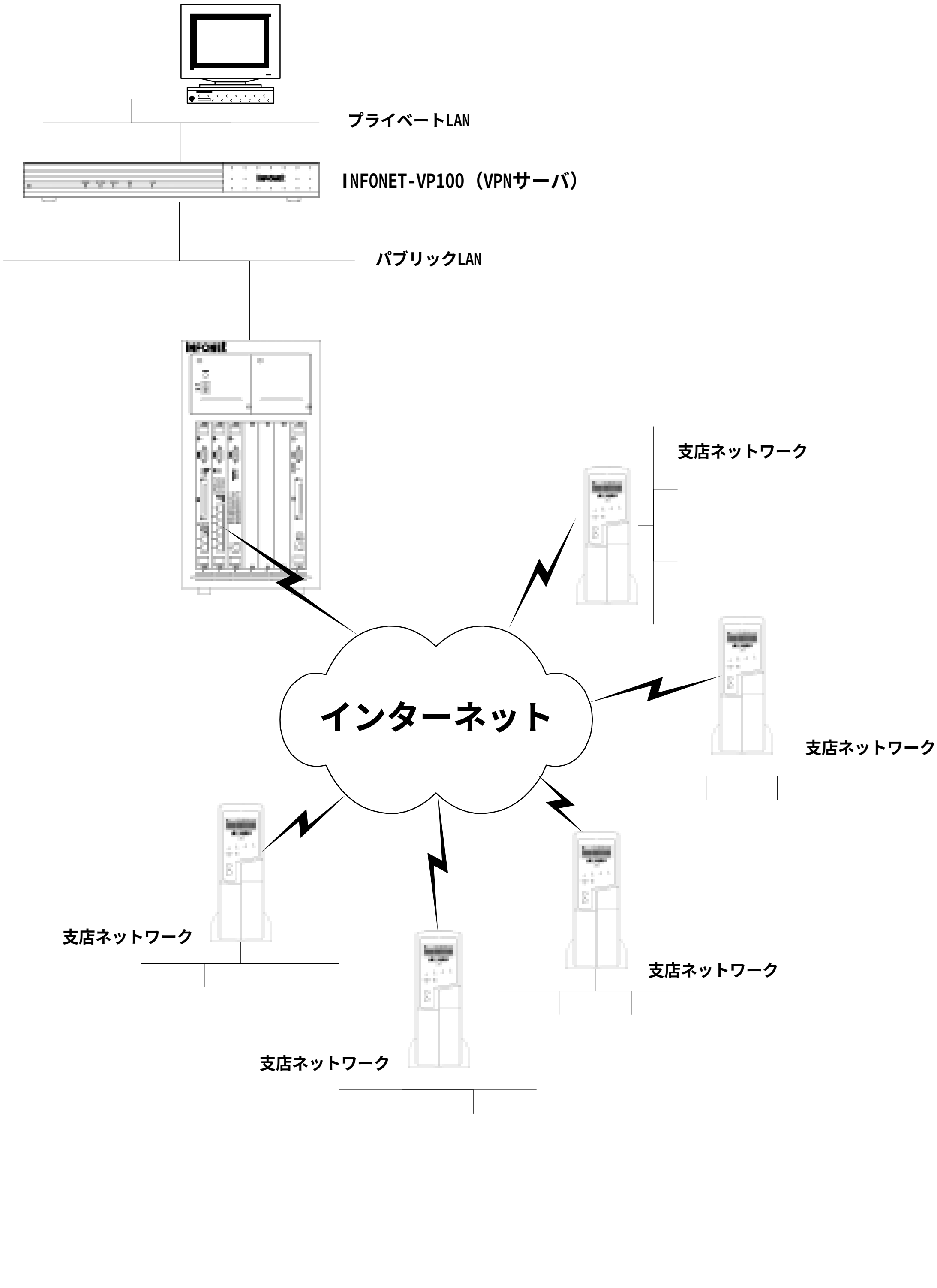
LED	動作
POWER（緑）	電源投入中を示し，通電中は点灯する.
CHECK（橙）	装置を運用上で，何らかの障害が発生した場合点滅する.
SYSTEM（緑）	ファームウェアの運用状態を示す.
PRIVATE（緑） PUBLIC（緑）	LAN の状態を示す
	点灯：正常運用 点滅：データの送受信があった時

2 機能概要

本章では，本装置で行える機能の概要を説明します.

2.1 本装置の位置付け

本装置は，遠隔地（支店）のルータと，IPsec の通信を行うことができる，IPsec サーバです.ネットワーク環境における，本装置の位置付けは，以下のネットワーク環境図で表すことができます.



INFONET-VP100 は，センター（本社）側のパブリック LAN／プライベート LAN の間に配置し，以下の機能を使用することができます.

（1）IP ルーティング機能 ・PRIVATE LAN と PUBLIC LAN を中継するルータとして使用します.ルーティングプロトコルには，RIP/RIPv2，スタティックルーティングを使用できます．本装置のルーティングテーブルは 3000 エントリです（スタティック含む）.

（2）IPsec 機能 ‥‥‥‥‥ 多拠点の営業所等と，IPsec の通信を行うことができます．IPsec を使用すると，開放されたネットワーク（インターネット等）内を，暗号化したデータで通信できるため，セキュリティを確保したデータ通信が可能になります.

（3）NAT/NAT+機能‥‥‥‥ プライベート LAN⇔パブリック LAN でのアドレス変換を行い，インターネット等外部にプライベートアドレスを見せなくすることができます.

（4）DHCP サーバ機能 ‥‥‥ プライベート LAN にダイナミックに IP アドレスを割当てることができます．この機能を利用すると，プライベート LAN に接続されている端末に IP アドレスを設定しなくても，IP 通信を行えるようになります.

（5）各種ログ機能および障害通知機能
‥‥‥‥‥‥‥‥ プライベート LAN への不正なアタックや，TELNET によるアクセスイベント等をログとして保存し，その情報を syslog や SNMP を使用して通知することができます.

次ページより，各種機能概要を説明します.

2.2 IPルーティング機能

本装置は，IP パケットのルーティング機能をサポートしています．本装置の IP ルーティング機能で，RIP(Routing Information Protocol)および RIP Version 2 を利用したダイナミックルーティングを利用したダイナミックルーティングとスタティックルーティングを併用して運用することができます．また接続相手によりネットワークの形態（以降インタフェースタイプ）を選択して運用することができます．

2.2.1 RIP および RIP Version 2 を利用したダイナミックルーティング

本装置は，RIP および RIP2 によるダイナミックルーティング機能をサポートしています．この機能により,本装置の持っているルーティング情報を RIP および RIP2 でネットワークへ広告します．また，RIP および RIP2 で獲得したルーティング情報によってルーティングテーブル（最大 3000 エントリ）の更新を行います．

ダイナミックルーティングは，ルータ間でルーティング情報の交換を行い，経路を決定する方法です．ルータ間の情報交換により経路を決定しますので，ルータの故障やネットワークの故障を発見し，常に最適な経路をダイナミックに選択できます．

2.2.2 スタティックルーティング

本装置は，ルーティング情報を設定により有効にするスタティックルーティングをサポートしています．

スタティックルーティングは，装置に設定された経路情報に従って経路を決定する方法です．

2.2.3 ダイナミックルーティングとスタティックルーティングの関係

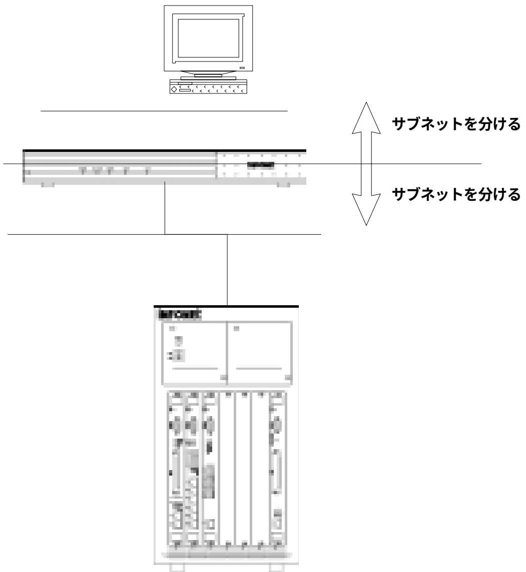
同じ宛先への経路が，ダイナミックルーティングで獲得したルーティング情報と，スタティックルーティングにより設定したルーティング情報で異なる場合，本装置ではどちらの情報を有効にするかを選択することができます．

メモ：同じ宛先への経路が，ダイナミックルーティングで獲得したルーティング情報と，スタティックルーティングにより設定したルーティング情報で異なる場合，それぞれの持つ優先度（ 「preference」値）によりどちらの情報を有効にするかを決定します．本装置では，スタティックルーティングの「preference」値を設定することができます（RIP は固定）．「preference」値が同じ場合には，宛先へ到達するために経由するルータの数（メトリック値）の少ない経路を有効とします．

2.2.4　インタフェースタイプ

本装置は，インタフェースタイプとして以下の２通りをサポートしています．2 つのインタフェースタイプの違いを以下に示します．

【ブロードキャストインタフェース】

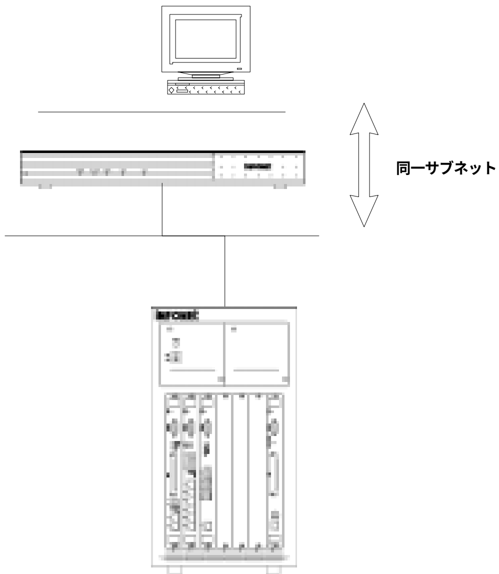


PRIVATE LAN と PUBLIC LAN でネットワークを切り分けます．PUBLIC LAN は外部ネットワークからアクセス可能，PRIVATE LAN はアクセス不可とするようなネットワーク形態を構築する場合は，ブロードキャストインタフェースとします．

⇩

PUBLIC LAN に割当てる IP アドレス／サブネットマスクを設定します．

【ポイントツーポイントインタフェース】



PRIVATE LAN と PUBLIC LAN で同一ネットワークとします．PRIVATE LAN も外部ネットワークからアクセス可能とするネットワーク形態を構築する場合は，ポイントツーポイントインターフェースとします．

⇩

相手インタフェースアドレス／サブネットマスクとして，外部ネットワークへの出口（図では INFONET-AX60）のアドレス／サブネットマスクを設定します．

2.2.5 Proxy ARP 機能

本装置は，サブネットの概念を持たない端末の ARP の要求に対して，装置自身の MAC アドレスを応答する機能（Proxy ARP 機能）をサポートしています．

本装置の Proxy ARP 機能は，以下の２通りがあります．

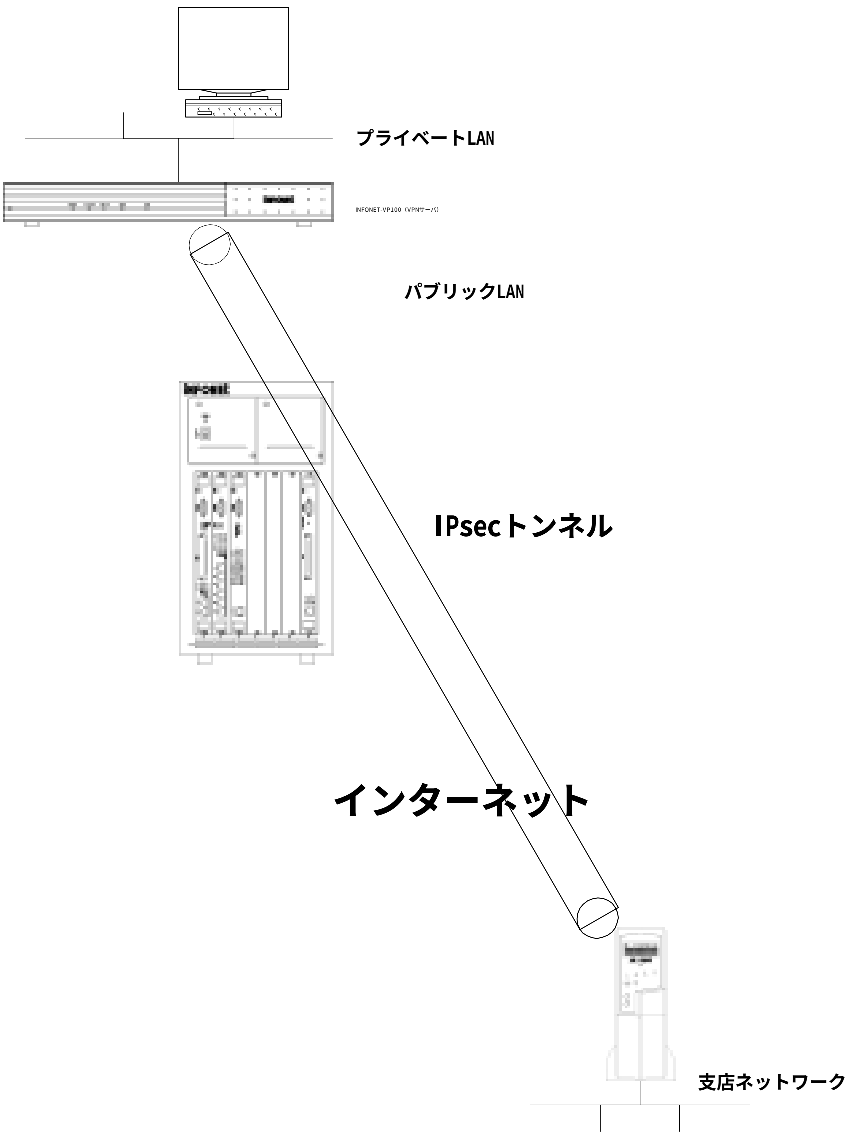
- **中継すべきアドレスへの ARP の要求に対して代理応答する．**
- **すべての ARP の要求に対して代理応答する．**

２．３ IPsec 機能（VPN）

IPsec とは，VPN（Virtual Private Network）の技術の一つです．VPN とは，インターネットのような開かれたネットワークを，あたかも専用線のような閉ざされたネットワークのように利用する技術です．

IPsec 機能は，接続相手と論理的な IPsec トンネルを形成し，トンネル内の IP データを暗号／復号する機能で，インターネットのような開かれたネットワーク上を通信する場合においても，改竄（かいざん）・盗聴などの危険から，大切なデータを守ることができる機能です．

本装置の暗号化アルゴリズムは DES-CBC 56bit,3DES-CBC　168bit,認証アルゴリズムは HMAC with MD5 または HMAC with SHA をサポートしています．また，鍵交換プロトコルは，IKE をサポートしています．



2.3.1 IPsecを使用するための設定

INFONET-VP100でIPsecを使うために必要な設定には，以下のようなものがあります.

①：VPNピアの登録

IPsecを使用して通信する接続相手ルータ(VPNピア)を登録します.支店と本社間をIPsec通信する場合には，お互いのルータを登録します．また，登録したVPNピアと鍵交換する際の，鍵データも設定します.

②：ポリシーの設定

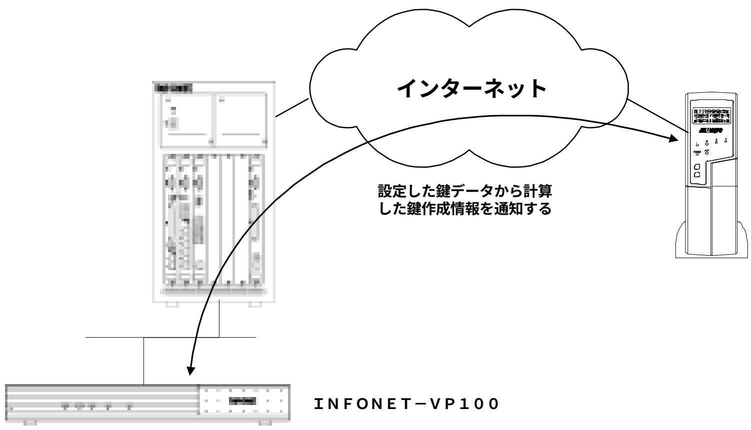
どのような条件でIPsec（暗号化・認証・鍵交換）を行うかを設定します．暗号アルゴリズム（DES or 3DES or 使用しない），認証アルゴリズム（HMAC-MD5 or HMAC-SHA or 使用しない）等の情報を設定します.

③：セレクタの設定

どのようなパケットに対してVPN制御を行うかを設定します．セレクタに登録した情報に一致したものをVPNで暗号化し，VPN通信を行います.

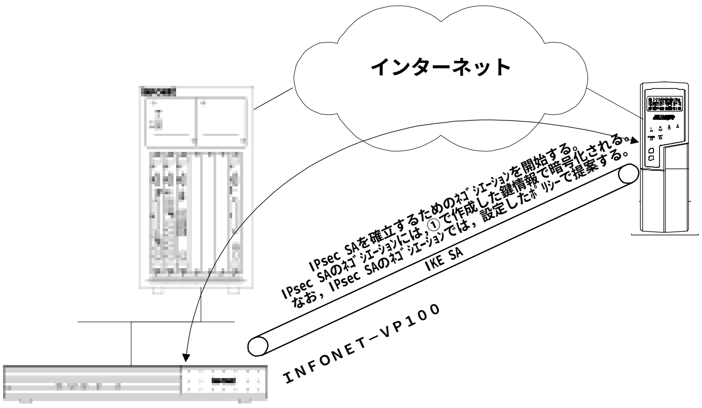
2.3.2 VPNの通信手順

① IKE SAの確立



pre-shared key方式の場合，設定した鍵データから計算した鍵作成情報をお互いに通知します．設定する鍵データは，IPsecを確立するどうしで同じでなくてはいけません.鍵作成情報が正しい場合（すなわち鍵データが正しい場合）にVPN通信を開始することができます（IKE SA確立）．IKE SAを確立した際は，鍵作成情報から鍵を作成します.複数の相手とVPN接続する場合には，相手毎の鍵が作成されます.
IKE SAは，設定したLifetime間後に消滅します

② IPsec SA の確立

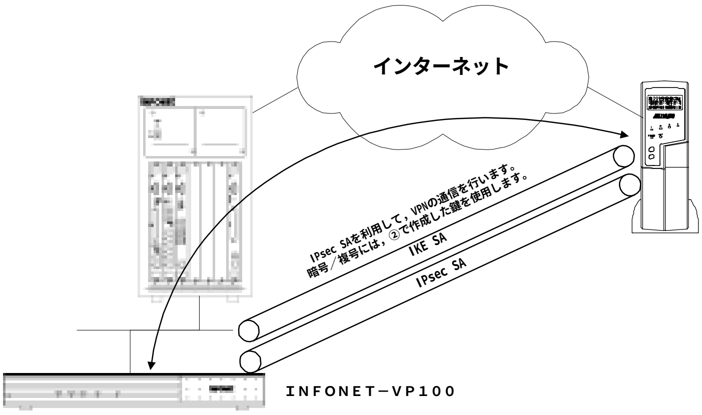


設定したセレクタに一致するパケットをPRIVATE LAN から受信した場合，セレクタで設定してある相手に対して，IPSEC SA を確立するためのネゴシエーションを開始します．IPsec SA のためのネゴシエーションには,①で作成された鍵を使用します．IPsec SA 通信では，指定したポリシーで提案します．指定したポリシーでネゴシエーションが拒否された場合，通信はできません．

IPsec SA を確立した際は，確立した IPsec SA を使用して通信する際の鍵が作成されます．

IPsec SA は，設定した Lifetime 間後に消滅します．消滅した後は再度，ネゴシエーションを行います．

③ 暗号化



設定したセレクタに一致するパケットをPRIVATE LAN から受信した場合，そのデータを暗号化します．暗号化は IPsec SA で確立したポリシーにしたがい，②で作成した鍵を使用します．データを暗号化することにより，盗聴されても判別できなくなります．データを複号する際も，②で作成した鍵を使用して複合します．

2.3.3 RSA signatures機能

RSA signatures機能とは，RSA方式の公開鍵／秘密鍵を使った電子署名を使うIKEでの認証方式です．メッセージダイジェスト（MD5などのハッシュ関数で作ったもの）をRSA秘密鍵で暗号化したものを署名とし，メッセージに添付します．

署名を利用することにより，従来のPre-Shared Key方式と比べて事前にPre-Shared Keyを設定する必要が無いため，よりセキュリティーを強固にすることができます．

さらに，Pre-Shared Key方式では，クライアントの数と同数のPre-Shared Keyをサーバー側に登録する必要があり，Pre-Shared Key の管理などの負荷が大きくなるが，RSA signatures機能では自分の秘密鍵を管理しておけば良く，大規模なネットワークでのスケーラビリティに優れています．

2.3.4 電子証明機能

RSA signatures機能を使用するためには，電子証明書の登録が必要であり，以下の機能を利用します．

- **鍵ペアの生成**
- **証明書使用時のパラメータの設定**
- **証明書リクエストの生成**
- **証明書の登録**

２.３.５　用語集

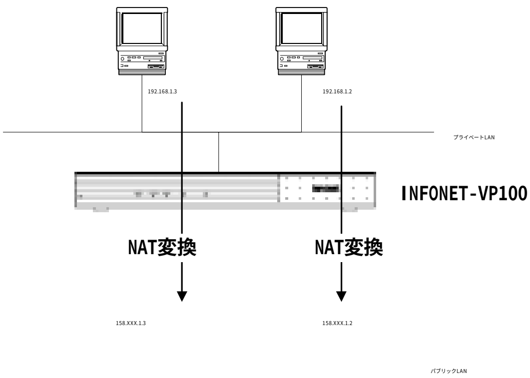
SA	Security Association の略．VPN 通信するための相手と確立する論理的なコネクション．SA には，暗号アルゴリズム・認証アルゴリズム等のセキュリティ情報を含んでいる
IKE	自動鍵管理プロトコル（RFC2409）．通信相手とのネゴシエーションにより自動で鍵を交換し SA を確立する方式.
Pre-Shared Key	自動鍵管理プロトコルでの鍵交換を行う際の，認証方法の一つ．共通鍵方式
RSA signatures	自動鍵管理プロトコルで鍵交換を行う際の，認証方法の一つ. RSA 公開鍵暗号方式による電子署名を使用する認証方法．公開鍵方式
CRL	証明書取り消しリスト
ISAKMP	IKE を実現するためのプロトコル．ISAKMP で， 「暗号アルゴリズム（DES-CBC）」， 「ハッシュアルゴリズム（MD5 or SHA-1）」， 「認証方法（pre-shared keys）」， 「Oakley Group description（Default 768-bit MODP group(group1)）」， 「鍵 Lifetime 秒」 「鍵 Lifetime バイト長」 の交換を行う. これらの情報をまとめて「ポリシー」という.
Diffie-Hellman	共通鍵交換方式で，第三者に盗聴されることなくかぎ交換を行うしくみ. ISAKMP でかぎ交換を行う際に使用している.
initiator	VPN ネゴシエーションを行う側
responder	VPN ネゴシエーションを受ける側
HMAC-MD5	認証アルゴリズムの一つ
HMAC-SHA	認証アルゴリズムの一つ
AH	Authentication Header. 旧 IPsec で規定されていた認証方法. INFONET-VP100 ではサポートしていない.
ESP	Encapsulation Security Payload（RFC2406）．IPsec で規定されている認証・暗号の方式．INFONET-VP100 では， 暗号アルゴリズムとして， ・DES-CBC 56bit ・NULL Encryption（暗号化しない） ハッシュアルゴリズムとして， ・HMAC with MD5 ・HMAC with SHA をサポートしている.

2.4 NAT/NAT+機能

本装置は，NAT/NAT+機能（Network Address Translator）をサポートしています．

【NAT 機能】

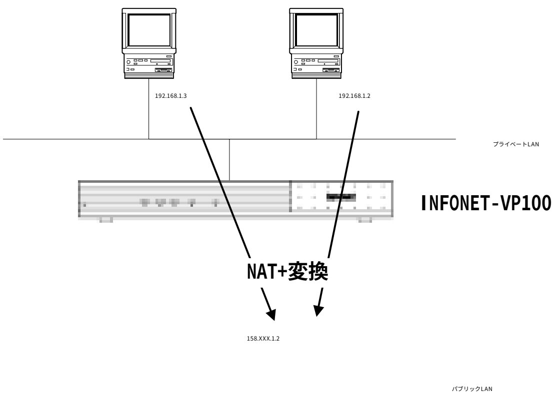
NAT（Network Address Translator）機能は，プライベート LAN に接続している端末の IP アドレスを，グローバル IP アドレスに変換することで，既存のプライベート IP アドレスを変更することなくインターネットに接続できる機能です．



【NAT+機能】

NAT 機能でのアドレス変換は 1 対 1 であるため，複数端末から同時に接続する場合には，複数のグローバル IP アドレスが必要となります．

NAT+機能では，複数端末のアドレスを，1 つのグローバル IP アドレスに集約することができます．この機能を利用すると，パブリック LAN の IP アドレスを本装置に 1 つ割当てるだけで，プライベート LAN の複数の端末がインターネット等外部ネットワークに接続することができるようになります．



また，NAT/NAT+機能を使用することにより，プライベート LAN の IP アドレスを外部に見せなくできるため，プライベート LAN のセキュリティも確保することができます．

２.５ DHCP サーバ機能

本装置は，DHCP サーバ機能をサポートしています．

DHCP（Dynamic Host Configuration Protocol）とは，DHCP サーバと DHCP クライアントから構成され，DHCP クライアント（パソコン等）の新設や移設時に，DHCP サーバがクライアントに PC の IP アドレスを自動的に割り付けるためのプロトコルです．

INFONET-VP100 では，上記 DHCP サーバ機能をサポートしています．これにより，パソコン等のネットワーク管理のめんどうな設定が不要となります．

割り付けられる項目は以下の通りです．

① 端末のアドレス
② デフォルトゲートウェイ（ルータのアドレス）
③ ドメイン名称
④ DNS（ドメインネームサーバ）のアドレス
⑤ WINS サーバのアドレス

INFONET-VP100 の DHCP サーバ機能では，端末に割り当てる IP アドレスの範囲を指定することもできます．

メモ：パソコン等でインターネットに接続する場合，DHCP を使用しないと，最低でも上記①～④の設定がパソコン等に必要です．

2.6 障害監視／通知機能

本装置では，装置やネットワークの障害を管理装置から管理する，あるいは障害の情報を管理装置に通知する機能を持っています．本装置の障害監視／通知機能には，以下の3種類があります．

- SNMP（Simple Network Management Protocol）を使用した障害監視／通知
- syslogdへの障害通知

2.6.1 SNMPを使用した障害監視／通知

SNMP（Simple Network Management Protocol）を使用して，本装置の監視・運用・障害通知を行うことができます．本装置では，SNMPマネージャを４エントリ登録することができます．

2.6.2 syslogdへの障害通知

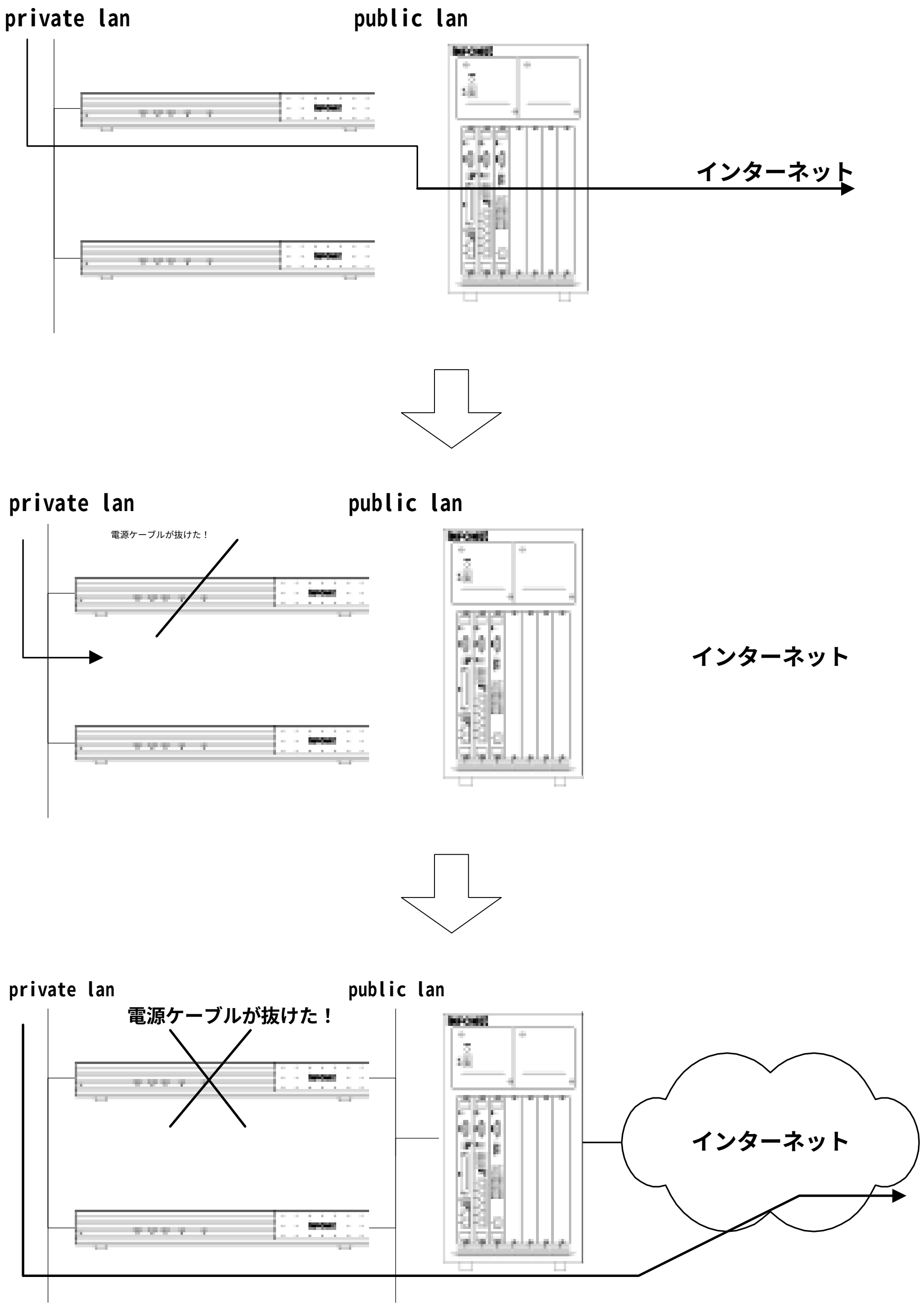
syslogd の動作している端末に，本装置のエラー情報等を送信することができます．送信する内容は，本装置のコンソールで参照できる「エラーログ」「ラインログ」「トラップログ」です．

２．７ RGRP 機能（バックアップ機能）

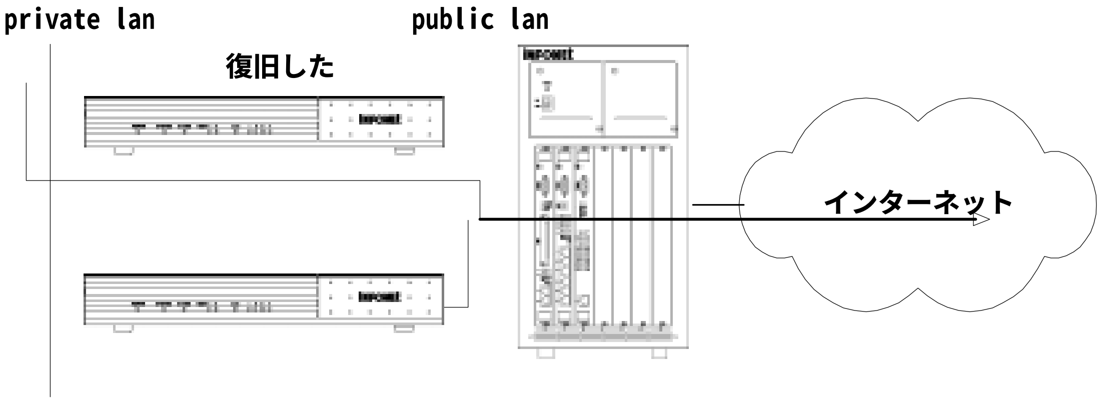
遠隔地を結ぶネットワークでは，ルータに何らかの障害が発生しただけで，全てのネットワークに支障をきたし，大切なデータを失ってしまうことにもなりかねません.

本装置では, INFONET-VP100 に障害が発生した場合に, 直ちに別の INFONET-VP100 を代替として, ネットワークに支障をきたさない機能（RGRP 機能）をサポートしています.

RGRP 機能では，別の INFONET-VP100 を経由することになっても，LAN に接続した端末の設定を変更する必要はありません.

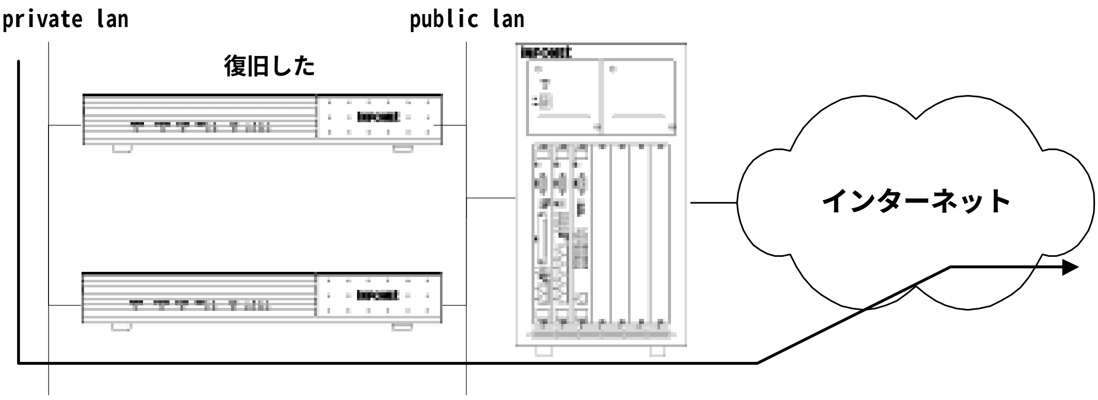


・ 障害があったルータが Owner だった場合
・ 障害があった INFONET－VP100 の先制モードが ON で，プライオリティがバックアップルータより高い場合



【復旧したらもとの経路に戻る】

・ 障害があった INFONET－VP100 の先制モードが OFF，あるいは先制モードが ON でプライオリティがバックアップルータより低い場合



【復旧しても経路は変更なし】

故障等が発生した INFONET-VP100 と，代替として動作する INFONET-VP100 とは，RGRP のグループを形成する必要があります．このグループを RGRP グループといいます．本装置では，最大４つの RGRP グループに属することができます．

なお，本書では，RGRP グループの中で実際にデータ転送するルータを Master ルータと記述します．

設定については，P１１-1を参照してください．

3　設定を始める前に

この章では，本装置の設定を行うためのコンソールの接続方法を紹介します.

- 装置の設定方法
- TELNET ログイン
- RCIP ログイン
- Normal/Super モード
- コンソールのタイムアウト
- 現在時刻の設定
- 装置のリセット方法
- パスワードの設定
- 本装置のコンソール画面

3.1 装置の設定方法

本装置の各種機能を設定するためには，以下に示す３通りの設定方法があります.

（１）Web ブラウザからの設定

（２）ローカルコンソールからの設定

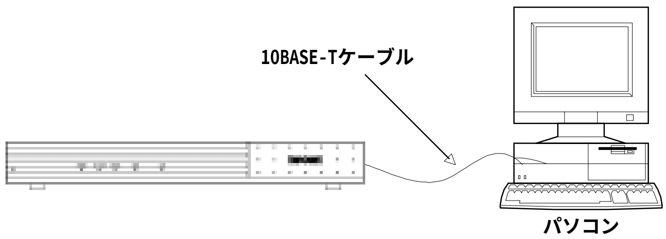
（３）TELNET でログインして設定

3.1.1 Web ブラウザからの設定

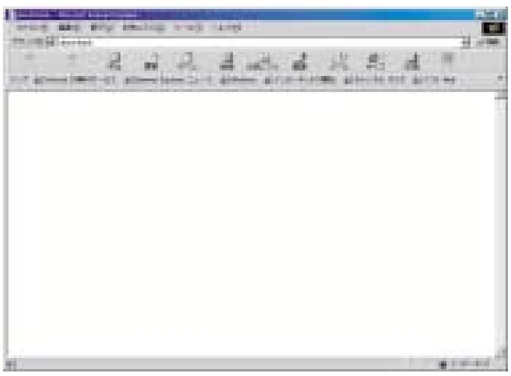
パソコンにインストールされている Web ブラウザソフト（Internet Explorer/Netscape Navigator）を使用して，本装置の設定を行うことができます.

Web ブラウザから設定を行う場合は，以下の手順で行ってください.

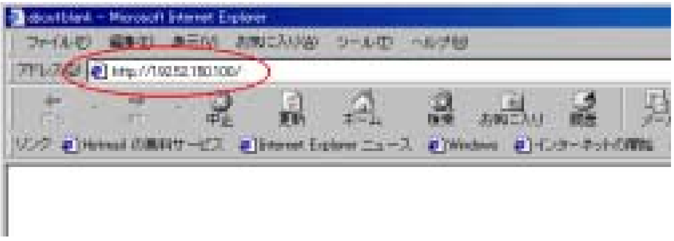
（１） 本装置とパソコンの LAN ポートを 10BASE-T ケーブル（別売）で接続します．本装置側は，PRIVATE LAN のポートにケーブルを接続してください．



（２） パソコンの Web ブラウザソフトを起動します



（3）http://192.52.150.100 にアクセスします．



（4）設定画面が表示されます．

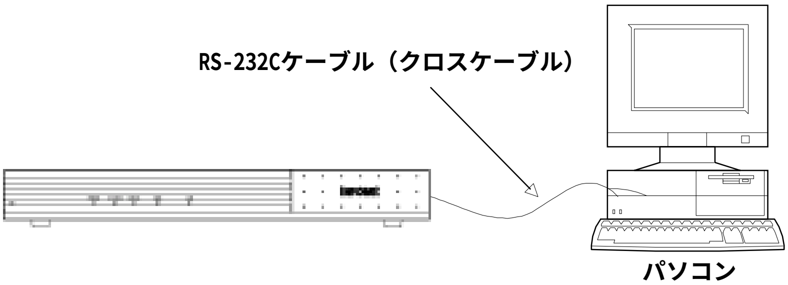
（5）メニュー画面から設定したい項目をクリックし，設定を行います．

3.1.2　ローカルコンソールからの設定

本装置と，ターミナルエミュレータソフト（hyperterm 等）が動作するパソコンを，RS-232C ケーブル（クロスケーブル）で直接接続し，システム編集および運用操作等を行うことができます．

Web ブラウザから設定を行う場合は，以下の手順で行ってください．

（1）　本装置とパソコンの COM ポートを RS-232C ケーブル（別売）で接続します．RS-232C ケーブルは，クロスケーブルを使用してください．



（2）パソコンでターミナルエミュレータソフト（ハイパーターミナル等）を起動します．

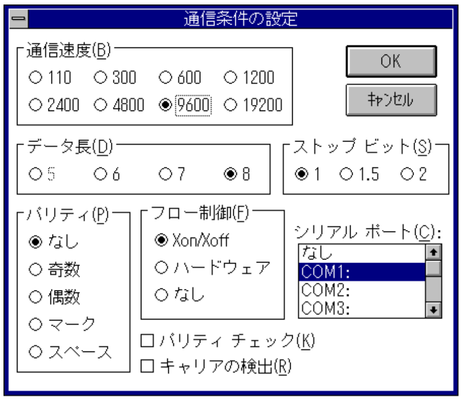
ターミナルエミュレータソフトの設定は以下のようにしてください．

ﾋﾞｯﾄ/秒／通信速度	9600
ﾃﾞｰﾀﾋﾞｯﾄ／データ長	8
ﾊﾟﾘﾃｨ／パリティ	なし
ｽﾄｯﾌﾟﾋﾞｯﾄ／ストップビット	1
ﾌﾛｰ制御／フロー制御	Xon/Xoff

HyperTerm（Windows95）の場合



Terminal（Windows3.1）の場合



（3）本装置を起動します．

（4）ログインパスワードを入力します．

入力するパスワードは表示されません．また，カーソルも動きません．初めてお使いになる時は，パスワードは設定されていません．【Enter】キーを押してください．

```
Login password:
```

（5）プロンプトが表示され，コマンド入力待ち状態になります．

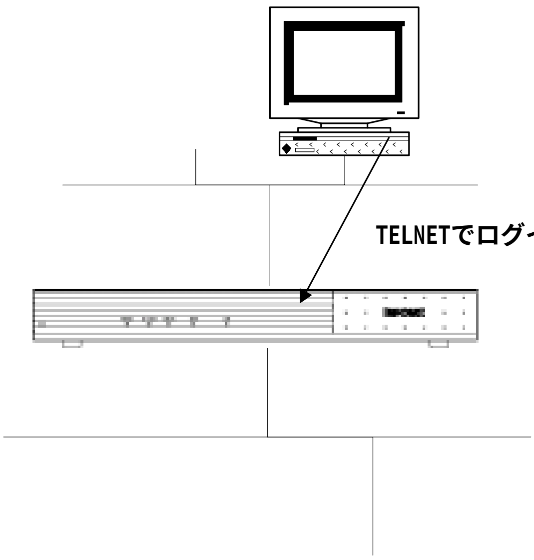
```
#
```

（6）設定を行う場合は，コンフィグレーションモードに移行します．

コンフィグレーションモードへの以降の仕方は，P３-7を参照してください．

3.1.3　TELNETでログインして設定

本装置は，TELNETサーバ機能をサポートしています．遠隔のTELNETクライアントからネットワークを経由して本装置にログインし，システム編集および運用操作等，ローカルコンソールと同等の操作を行うことができます．ログインした後は，ローカルコンソールと同じ方法で操作します．



3.2 モードの移行

本装置では，以下の2つのモードがあります．

（1）ログインモード

（2）コンフィグレーションモード

3.2.1 ログインモード

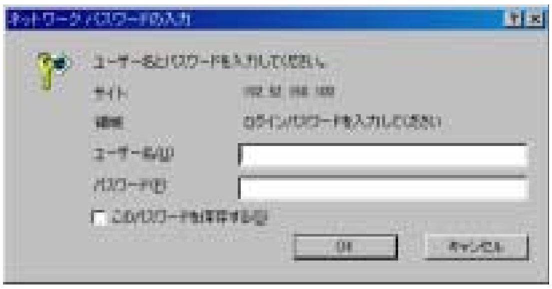
ログインモードでは，装置の運用･操作・情報表示を行うことができます．このモードでは設定を行うことができません．

ログインモードに移行するためには，ログインパスワードが必要です．ログインパスワードの設定方法はP3-12を参照してください．なお，初めてお使いになる時は，パスワードは設定されていません．

ログインモードへの移行方法を以下に示します．

（1）Webブラウザから操作している場合

Web ブラウザ画面で，装置の運用・操作・情報表示に該当するリンクを選択した際に，以下の画面が表示されます．このとき，ユーザ名には"root"，パスワードにログインパスワードを入力します．この入力により，ログインモードに移行でき，以降運用･操作･情報表示を行うことができます．



ログインモードを終了する際は，Webブラウザ画面を終了してください．

（2）コンソールから操作している場合

コンソールを接続して起動した際，コンソールに以下の画面が表示されます．

```
Login password:
```

この画面で，ログインパスワードを入力することにより，ログインモードに移行し，コマンド入力待ち状態になります．

ログインモードを終了する際は，exitコマンドを入力してください．

```
# exit
```

（3）TELNETでログインして操作する場合

TELNETでログインする際にパスワードの問合せがあります．ログインパスワードを入力することにより，ログインモードに移行します．

3.2.2　コンフィグレーションモード

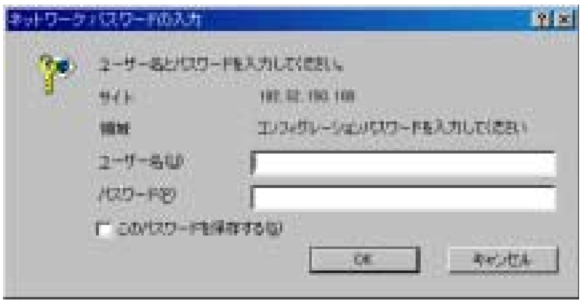
コンフィグレーションモードでは，本装置の各種設定を行うことができます．

コンフィグレーションモードに移行するためには，コンフィグレーションパスワードが必要です．コンフィグレーションパスワードの設定方法はP３-12を参照してください．なお，初めてお使いになる時は，パスワードは設定されていません．

コンフィグレーションモードへの移行方法を以下に示します．

（1）Webブラウザから操作している場合

Web ブラウザ画面で，設定に該当するリンクを選択した際に，以下の画面が表示されます．このとき,ユーザ名には"root",パスワードにコンフィグレーションパスワードを入力します．この入力により，コンフィグレーションモードに移行でき，設定を行うことができます．



コンフィグレーションモードを終了する際は，Webブラウザ画面を終了してください．

（2）コンソールから設定する場合

コンフィグレーションモードに移行するには，まずログインモードに移行します．ログインモードへの移行方法は，P３-6を参照してください．

ログインモードのプロンプトで，"config"と入力し，コンフィグレーションパスワードを入力することにより，コンフィグレーションモードに移行することができます．

```
# config  ←"config"コマンドを入力
Configuration password:  ←コンフィグレーションパスワードを入力
conf#  ←コンフィグレーションモードに移行
```

コンフィグレーションモードを終了する際は，exitコマンドを入力してください．ログインモードに移行します．

```
conf# exit
```

（3）TELNETでログインして設定する場合

TELNETでログインした後は，コンソールから設定する場合と同じです．

3.3 コンソールタイムアウト機能

本装置では，装置のセキュリティ等を考慮し，コンフィグレーションモード／ログインモードにおいて５分間何も操作が行われなかった場合，自動的にログアウトされます.

お知らせ

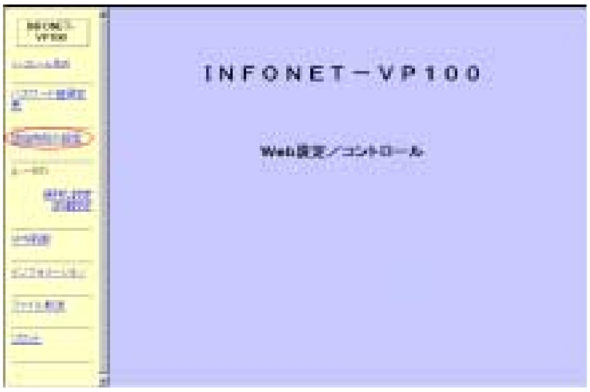
設定中に，5 分間操作が行われず自動的に一般設定に戻った場合，それまで行った設定は無効になります.

3.4 現在時刻の設定

本装置では，IPsec で使用する SA を指定時刻に確立しなおしたり，ログの表示時間を明記するために，現在時刻を管理しています．装置導入時には，現在時刻が設定されていますが，変更が必要な場合は，Web ブラウザまたはコンソールから変更することができます.

3.4.1 Web ブラウザからの設定

Web ブラウザから，本装置にアクセスした画面で，現在時刻の設定を選択し，現在の日時を設定します．現在時刻を設定した後，「送信」ボタンを押します.



初期画面で「現在時刻の設定」をクリックします.



現在時刻を設定した後「送信」をクリックします.

3.4.2　コンソールからの設定

コンソールまたはTELNETで，本装置にログインし，ログインモードで"date"コマンドにより現在時刻を設定します．

dateコマンドの書式は，

date 年月日.時分秒です．

```
#date 000816.140000
```

上記の例では，2000年8月16日 14時00分00秒に設定した場合の例です．

本設定は，設定したと同時に有効になります．

３．５ 装置のリセット方法

本装置のリセット方法には，以下の３つの方法があります．

（１）本装置の裏面にあるリセットスイッチの押下

（２）Web ブラウザより，リセット発行

（３）コンソールより，リセットコマンドを発行

３．５．１　リセットスイッチの押下

リセットスイッチを押下する場合は，本装置裏面にあるリセットスイッチを，先の尖ったもので押してください．

３．５．２　Web ブラウザからのリセット発行

Web ブラウザから，本装置にアクセスした画面で，「リセット」を選択し，リセット画面に移行後「装置をリセットする」にチェックをしたあと，「送信」ボタンを押します．



初期画面で「リセット」をクリックします．



「装置をリセットする」を選択した後「送信」をクリックします．

3.5.3　コンソールからのリセットコマンド発行

コンソールまたは TELNET で，本装置にログインし，ログインモードで"reset"コマンドにより装置をリセットします．

```
#reset
Do you want to continue (y/n)?: y
```

3.6 パスワードの設定

本装置では，ログインモード／コンフィグレーションモードに移行するために，パスワードの入力が必要となります．

装置導入時は，パスワードが設定されていません．

パスワードの変更は，Web ブラウザまたはコンソールから変更することができます．

3.6.1 Web ブラウザからパスワード変更

Web ブラウザから，本装置にアクセスした画面で，「パスワード登録変更」を選択し，ログインパスワードを変更する場合は「ログインパスワード」，コンフィグレーションパスワードを変更する場合は「コンフィグレーションパスワード」を選択します．表示された画面で，「旧パスワード」に現在のパスワードを，「新パスワード」と「確認の為，新パスワードを再度入力して下さい」に新しく設定するパスワードを入力します．全てを入力した後，「送信」ボタンを押します．



初期画面で「パスワード登録変更」をクリックします．

⇩



登録変更パスワードの選択画面で登録，変更を行いたいパスワードを選択します．

※これより，ログインパスワードの登録変更を例に説明します．

⇩



パスワード設定後，「送信」をクリックします．.

※装置導入時は，パスワードが設定されていませんので，「旧パスワード」は空白にします．

3.6.2　コンソールからのパスワード変更

コンソールまたはTELNETで本装置にログインし，ログインモードで"password"コマンドによりパスワードを変更します.

ログインパスワードを変更する場合は"password"，コンフィグレーションパスワードを変更する場合は"password -c"と入力します.

【ログインパスワードの変更】

```
#password
old password:          ←現在のログインパスワードを入力
new password:          ←新しく設定するのログインパスワードを入力
retype new password:  ←新しく設定するのログインパスワードを再入力
#
```

【コンフィグレーションパスワードの変更】

```
#password -c
old password:          ←現在のコンフィグレーションパスワードを入力
new password:          ←新しく設定するのコンフィグレーションパスワードを入力
retype new password:  ←新しく設定するのコンフィグレーションパスワードを再入力
#
```

メモ：装置導入時は，パスワードが設定されていませんので，"old password"の問合せはありません．

4　LAN について

この章では，本装置を LAN に接続する際の注意点を紹介します．

－　LAN への接続方法

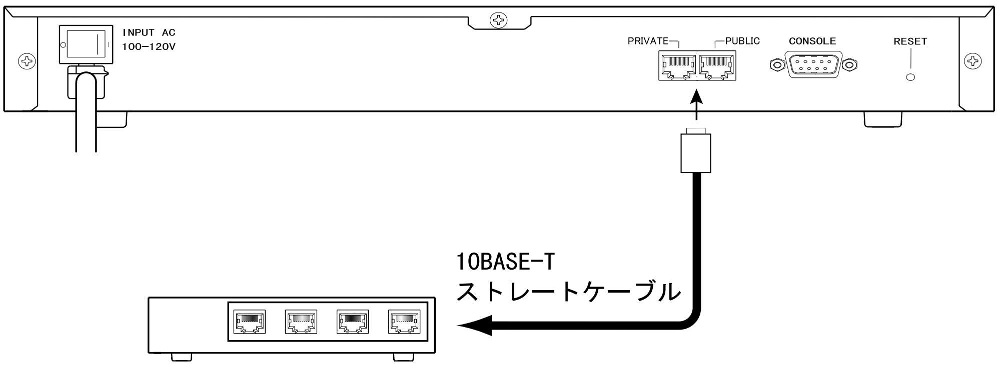
－　接続確認方法

4.1 LAN への接続

本装置を LAN に接続するには，HUB を介してネットワークへ接続します.
以下に接続方法を説明します.

HUBに接続

本装置と HUB を接続する場合，接続に使用するケーブルは 10BASE-T ストレートケーブルを使用してください.



4.2 LAN の接続確認

LAN に接続した場合の，接続確認方法を示します.
本装置の LAN ポートと，HUB の任意のポートを接続し HUB のリンクランプが点灯した場合，正常に通信が出来る状態です.
リンクランプが点灯しない場合は，接続に使用している 10BASE-T ケーブルがストレートであることをご確認ください.

5　IP ルーティングに関する設定

5.1 設定方法

IP ルーティングするために，Web ブラウザおよびコンソールを使用して，具体的に設定を行う方法について説明します．設定の準備については，「3.1　装置の設定方法」を参照してください．

本項では，IP ルーティングに関する設定を，以下の分類に分けて説明します．

（1）本装置で IP ルーティングする場合に必ず設定する項目

（2）設定すると，より効率よくネットワークを運用できる項目

（3）通常はデフォルトで使用する項目

5.1.1　本装置で IP ルーティングする場合に必ず設定する項目

本装置で IP ルーティングする場合に，必ず設定する項目には，以下の項目があります．

【インタフェースの設定】

【RIP の制御】

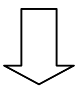
5.1.1.1　インタフェースの設定

PRIVATE LAN/PUBLIC LAN のインタフェースに割当てる IP アドレスを設定します．ここでは，Web ブラウザおよびコンソールから，インタフェースのアドレスを設定する方法について記述します．

（1）Web ブラウザからの設定



初期画面で「便利な設定」をクリックします．





ルータの便利な設定画面で「インタフェース」をクリックします．



インタフェースの設定画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

PRIVATE LANインタフェース：

インタフェースアドレス‥ PRIVATE LANのIPアドレスを設定します．装置導入時には，192.52.150.100が設定されています．

インタフェースサブネットマスク

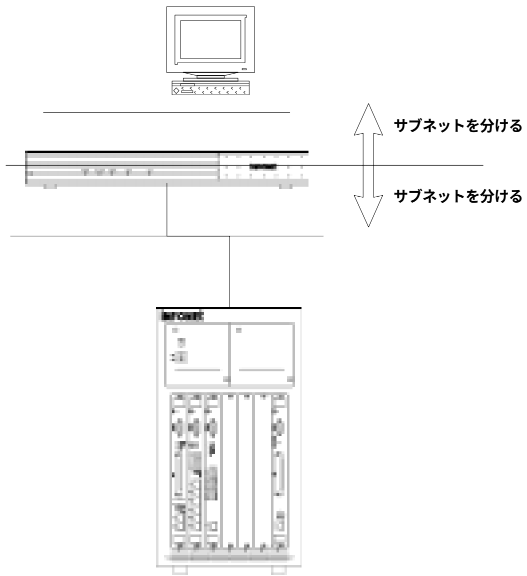
‥‥‥‥‥‥‥‥‥‥‥‥ PRIVATE LANのサブネットマスクを設定します．装置導入時には，255.255.255.0が設定されています．

PUBLIC LANインタフェース：

ダウン／ブロードキャスト／ポイントツーポイント　ラジオボタン

‥‥‥‥‥‥‥‥‥‥‥‥ PUBLIC LANのインタフェースタイプを選択します．
PUBLIC LANインタフェースを使用しない場合は「ダウン」，ブロードキャストインタフェースとする場合は「ブロードキャスト」，ポイントツーポイントとする場合は「ポイントツーポイント」をチェックします．ブロードキャストインタフェースとポイントツーポイントインタフェースの違いを以下に示します．

【ブロードキャストインタフェース】

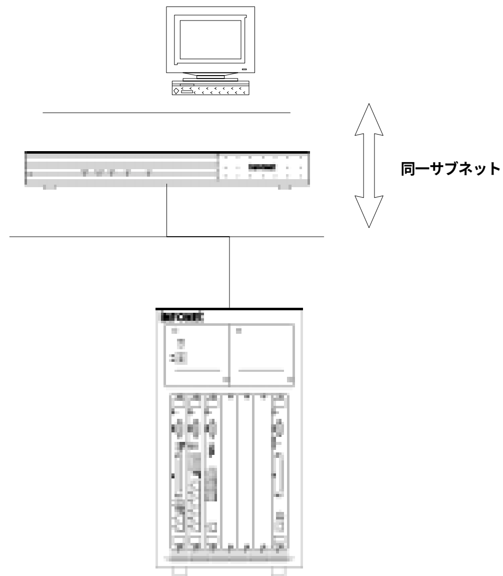


PRIVATE LAN と PUBLIC LAN でネットワークを切り分けます．PUBLIC LAN は外部ネットワークからアクセス可能，PRIVATE LAN はアクセス不可とするようなネットワーク形態を構築する場合は，ブロードキャストインタフェースとします．

↓

PUBLIC LAN に割当てる IP アドレス／サブネットマスクを設定します．

【ポイントツーポイントインタフェース】



PRIVATE LAN と PUBLIC LAN で同一ネットワークとします．PRIVATE LAN も外部ネットワークからアクセス可能とするネットワーク形態を構築する場合は，ポイントツーポイントインターフェースとします．

↓

相手インタフェースアドレス／サブネットマスクとして，外部ネットワークへの出口（図では INFONET-AX60）のアドレス／サブネットマスクを設定します．

（2）コンソールからの設定

コンソールより，interface コマンドで，インタフェースの IP アドレスの設定を行います．設定はコンフィグレーションモードで行います．

```
conf#interface ip private addr=192.52.150.100,255.255.255.0  ①
conf#interface ip public remote=192.52.150.1,255.255.255.0   ②
conf#interface ip public addr=158.XXX.1.100,255.255.0.0      ③
```

①： PRIVATE LAN の IP アドレスを，192.52.150.100，サブアドレスを 255.255.255.0 に設定しています．

②： PUBLIC LAN のインタフェースタイプをポイントツーポイント，相手側インタフェースの IP アドレスを 192.52.150.1, サブネットマスクを 255.255.255.0 に設定しています．

③： PUBLIC LAN のインタフェースタイプをブロードキャスト，PUBLIC LAN に割当てる IP アドレスを 158.XXX.1.100，サブネットマスクを 255.255.0.0 に設定しています．

【解説】

interface コマンドでは，インタフェースに割当てる IP アドレスを設定します．
PUBLIC LAN インタフェースについては，インタフェースタイプ（ブロードキャスト or ポイントツーポイント）も指定します．

①で，

　interface ip private addr=〜〜

と入力している「private」は PRIVATE LAN インタフェースを意味し，「addr=〜〜」は割当てる IP アドレスの定義を意味します．

②で，

　interface ip public remote=〜〜

と入力している「public」は PUBLIC LAN インタフェースを意味し，「remote=〜〜」はポイントツーポイントインタフェース／相手側インタフェースの IP アドレスの定義を意味します．

③で，

　interface ip public addr=〜〜

と入力している「public」は PUBLIC LAN インタフェースを意味し，「addr=〜〜」はブロードキャストインタフェース／割当てる IP アドレスの定義を意味します．

PRIVATE LAN の IP アドレスは，①のコマンド例を参考にして，設定してください．

PUBLIC LAN の IP アドレスは，②または③のどちらかのコマンド例を参考にして，ご利用のネットワーク環境に合うように設定してください．インタフェースタイプについては，P5-3 を参照してください

5.1.1.2　RIPの制御

RIP動作モードに関する設定を行います.

（1）Webブラウザからの設定



初期画面で「詳細設定」をクリックします.



ルータの詳細設定画面で「RIPの制御」をクリックします.



RIPの制御設定画面で，各種設定を入力した後に「送信」をクリックします．.

（2）コンソールからの設定

コンソールより，iprouting コマンドで，RIP の動作モードの設定を行います．設定はコンフィグレーションモードで行います．

```
conf#iprouting rip=on
```

【解説】

iprouting コマンドで，rip=on を指定することにより，RIP 動作します．RIP 動作を停止する場合は，rip=off を指定します．スタティックルーティングを行う場合は，スタティックルーティングテーブル（ipripstatic コマンド）を登録してください．

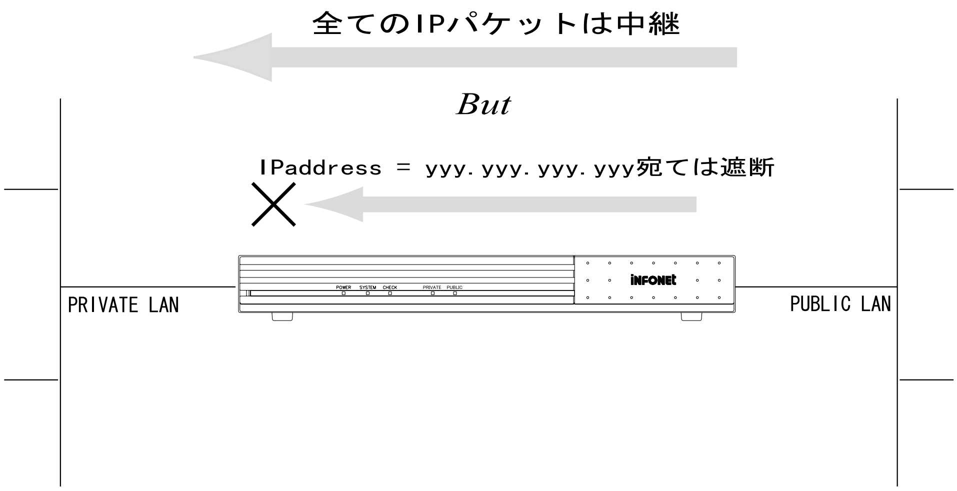
5.1.2　設定すると，より効率よくネットワークを運用できる項目

本装置で IP ルーティングする場合に，設定すると，より効率よくネットワークを運用できる項目には，以下の項目があります.

【パケットフィルタリング】
【スタティックルーティング】
【proxyARP】
【RIP のフィルタリング】
【ルート情報提供ルータの指定】

5.1.2.1　パケットフィルタリングの設定

本装置では，登録したパケットのみ中継／遮断する機能（IP パケットフィルタリング機能）を使用することができます．以下に使用例を示します.



図では，宛先の IP アドレスにより判断して，パケットを中継／遮断していますが，本装置では，他に以下のパラメータでもパケットを中継／遮断することができます.

【送信元アドレス】
【宛先アドレス】
【プロトコル（TCP or UDP）】
【上位ポート番号（FTP，TELNET 等）】
【受信・送信インタフェース】

本装置の IP パケットフィルタリング機能は，まず中継するパケットのエントリを指定し，その中から遮断するパケットのエントリを指定します.

次ページより，本機能を使用するための設定方法について説明します．本装置では，中継パケットを指定するエントリは最大６４エントリ，遮断パケットを指定するエントリは最大３２エントリ指定することができます.

（1）Webブラウザからの設定



初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「**IP**パケットフィルタリング」をクリックします.

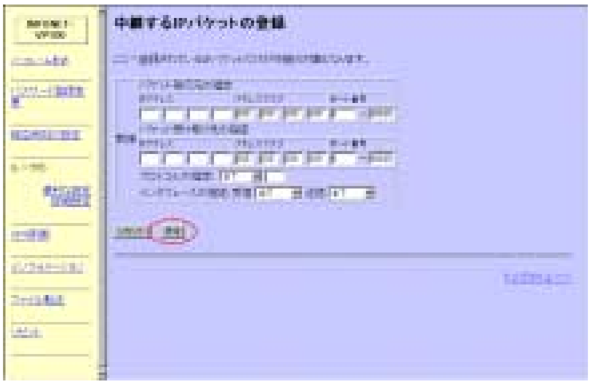


IPパケットフィルタリング設定画面で「IPパケットフィルタリング機能」にONを選択して,「送信」をクリックします.
さらに,「中継するIPパケットの登録を行う」「上記登録中から中継したくないIPパケットの登録を行う」をクリックし,フィルタリングの対象とするパケットを登録します.



新規に登録する場合は「新規登録」，すでに登録されている情報を変更する場合は，表中のエントリ番号をクリックします．

※ここでは，中継する IP パケットの登録を例に説明していますが，中継しない IP パケットの登録方法も同じです．



フィルタリングの対象とするパケットの，各設定値を入力し，「送信」をクリックします．

【パケット発行元の指定】

フィルタリングの対象とするパケットの送信元 IP アドレス／マスクパターン／ポート番号を入力します．

【パケット受け取り先の指定】

フィルタリングの対象とするパケットのあて先 IP アドレス／マスクパターン／ポート番号を入力します．

【プロトコルの指定】

フィルタリングの対象とするプロトコルを指定します（全て，TCP/UDP，ICMP，TCP，UDP，任意の中から選択）．「任意」を選択した場合は，プロトコル番号を指定します．

【インタフェースの指定】

フィルタリングの対象とする受信／送信インタフェースを指定します．

（2）コンソールからの設定

コンソールより，ipfiltering コマンドで，パケットフィルタリングの設定を行います．設定はコンフィグレーションモードで行います．

```
conf#iprouting filtering=on
conf#ipfiltering -f add dst=1.1.1.0,255.255.255.0 dstport=1,65535
src=2.2.2.0,255.255.255.0 srcport=1,65535 prot=all recvif=privatelan
sendif=publiclan  ①
conf#ipfiltering -d add dst=1.1.1.1,255.255.255.255 dstport=1,65535
src=2.2.2.2,255.255.255.255 srcport=1,65535 prot=all recvif=privatelan
sendif=publiclan                                                    ②
```

【解説】

ipfiltering コマンドで，中継／遮断するパケットを登録し，ルーティングするパケットを限定します．ipfiltering -f では中継を許可するパケットを，ipfiltering -d では中継を許可しない（遮断する）パケットを登録します．

本装置の IP フィルタリング機能を設定する際は，まず"ipfiltering -f"で中継を許可するパケットを登録し，その中から遮断するパケットを"ipfiltering -d"で登録します．遮断するテーブルのみ登録した場合は，全てのパケットが遮断されてしまうので注意してください．

上記設定例では，

「①2.2.2.0 → 1.1.1.0 のパケットは，PRIVATE LAN→PUBLIC LAN に中継する」

「②ただし 2.2.2.2 → 1.1.1.1 のパケットは，PRIVATE LAN→PUBLIC LAN に中継しない」

という設定になります．

ipfiltering コマンドの各パラメータについては，「INFONET-VP100　コマンドリファレンス」を参照してください．

5.1.2.2　スタティックルーティングの設定

ご利用になる LAN 環境に複数のネットワークがある時は，経路情報を設定することができます．中継するパケットを受信した場合，そのパケットを送り出す先の情報を設定します．本装置では，スタティックルーティングテーブルを，500 件登録できます．

（1）Web ブラウザからの設定



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「IP RIP スタティック」をクリックします．



ルータの便利な設定画面で新規に登録する場合は「新規登録」，すでに登録されている情報を変更する場合は，表中のエントリをクリック（表にはあて先アドレスが書かれています）します．



IP RIP スタティック設定画面で，各設定値を入力し，「送信」をクリックします．

（2）コンソールからの設定

コンソールより，ipripstatic コマンドで，スタティックルーティングの設定を行います．設定はコンフィグレーションモードで行います．

```
conf#ipripstatic add dst=1.1.1.0,255.255.255.0 nexthop=158.XXX.1.1
metric=1
```

【解説】

ipripstatic コマンドで，スタティックルーティングテーブルを登録します．

上記設定例では，

「①1.1.1.0 /255.255.255.0 への経路は，158.XXX.1.1 とする」

という設定になります．

ipripstatic コマンドの各パラメータについては，「INFONET-VP100　コマンドリファレンス」を参照してください．

５．１．２．３　 proxyARP の設定

proxyARP 動作モードに関する設定を行います.

（１）Web ブラウザからの設定



初期画面で「詳細設定」をクリックします.



ルータの詳細設定画面で「ProxyARP の設定」をクリックします.



ProxyARP の設定画面で，ProxyARP の動作を選択し，「送信」をクリックします.

（2）コンソールからの設定

コンソールより，iprouting コマンドで，proxyARP の動作モードの設定を行います.

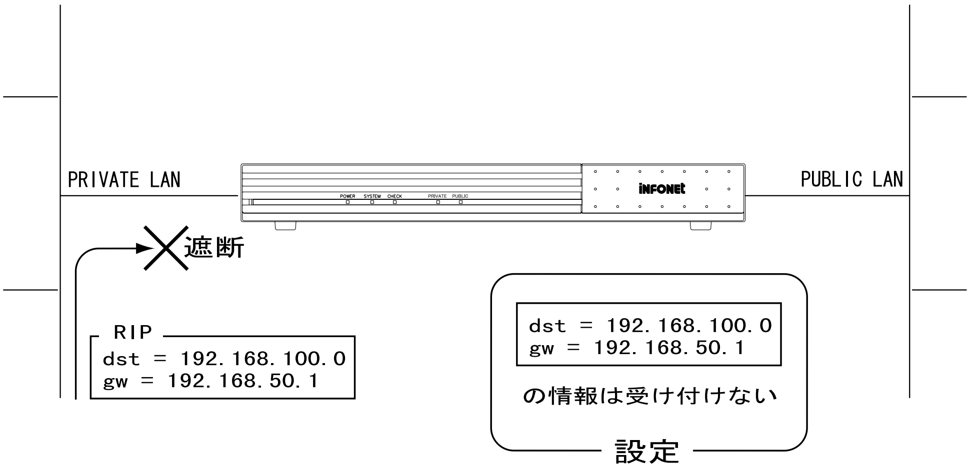
```
conf#iprouting proxyarp=shortcut
```

【項目の説明】

proxy・・・・・・・・・・・・・・・・・・・ proxyARP の使用方法を選択します.

off	：proxyARP 動作を行いません.
shortcut	：本装置がルーティングする必要のあるパケットに対してのみ自装置の MAC アドレスを応答します.
any	：本装置がルーティングする必要のないパケットに対しても自装置の MAC アドレスを応答します.

5.1.2.4　RIP のフィルタリング設定



本装置では，受信した RIP 情報を有効にするかどうか・RIP 情報として送信するかどうかを制御することができます.

図では，宛先・インタフェースの組み合わせを設定し，RIP 情報を受付けない（interface accept）としていますが，本装置ではこの他に以下の組み合わせがあります.

【宛先を設定し，その情報を RIP で送信する／しないインタフェースを設定（interface propagate）】

次ページより，本機能を使用するための設定方法について説明します. 【interface accept】，【interface propagate】はそれぞれ最大４０エントリ登録できます.

Web ブラウザからの設定



初期画面で「詳細設定」をクリックします．



ルータの詳細設定画面で目的に合わせ，「受信 RIP フィルタリングテーブル」または「送信 RIP フィルタリングテーブル」をクリックします．

※ここでは，受信 RIP フィルタリングテーブルを例に説明していますが，送信 RIP フィルタリングテーブルの登録方法も同じです．



新規に登録する場合は「新規登録」，すでに登録されている情報を変更する場合は，表中のエントリをクリックします．



受信 RIP フィルタリングテーブルの設定で，あて先 IP アドレス／マスク，受信インタフェースを設定し，送信をクリックします.

【RIP の宛先 IP アドレス】

受信ルーティング情報のフィルタリングの対象とする宛先 IP アドレスを入力します.

【アドレスマスク】

宛先 IP アドレスに対するマスクパターンを入力します.

【受信インタフェース】

受信インタフェースを選択します.

（2）コンソールからの設定

コンソールより，iprouting コマンドおよび ifaccept コマンドで，受信 RIP フィルタリングの設定を行います．設定はコンフィグレーションモードで行います.

```
conf#iprouting ifaccept=exclude  ①
conf#ifaccept add dst=192.168.1.0,255.255.255.0 recvif=privatelan  ②
```

【解説】

ifaccept コマンドで，受信 RIP フィルタリングテーブルを登録します.

上記設定例では,

「①受信 RIP フィルタリングテーブルに登録されている情報は受信しない」

「②PRIVATE LAN から受信する，192.168.1.0 /255.255.255.0 への RIP 情報をフィルタリングの対象とする」という設定になります.

①：ifaccept=exluce は，「受信 RIP フィルタリングテーブルに登録されている情報は受信しない」という設定になります．「受信 RIP フィルタリングテーブルに登録されている情報を受信する」とする場合には，ifaccept=include とします.

iprouting/ifaccept コマンドの各パラメータについては，「INFONET-VP100　コマンドリファレンス」を参照してください.

5.1.2.5　ルート情報提供ルータの指定

本装置では，有効なルーティング情報を提供してくれるゲートウェイ（trust gateway）の設定ができます．ここで設定する trust gateway 以外からの RIP 情報は有効としません．

以下に，trust gateway の設定方法を説明します．

Web ブラウザからの設定



初期画面で「詳細設定」をクリックします．



ルータの詳細設定画面で「ルート情報提供ルータの指定」をクリックします．



ルート情報提供ルータの指定画面で，trust gateway を登録し，「送信」をクリックします．

（2）コンソールからの設定

コンソールより，trustgateways コマンドで，ルート情報提供ルータの設定を行います．設定はコンフィグレーションモードで行います．

```
conf#trustgateways add nexthop=192.168.10.1 ①
```

【解説】

trustgateways コマンドで，ルート情報提供ルータを登録します．
上記設定例では，
「①192.168.10.1 をルート情報提供ルータとする」
という設定になります．
この場合，192.168.10.1 以外からの RIP 情報は受信しません．

6　IPsec 機能に関する設定

IPsec 機能を使用する場合は，はじめに，IKE の認証方式を設定する必要があります．

本装置は，IKE の認証方式に Pre-Shared key を使用する方式と，RSA signatures を使用する方法があります．

6.1　IKE ポリシーの登録

IKE ポリシーの登録時に，認証方式を選択することができます．

6.1.1　Web ブラウザからの設定

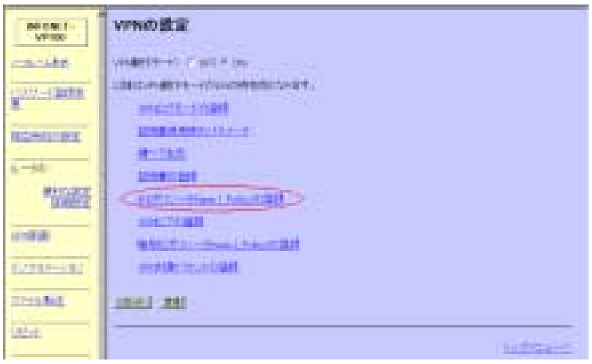
Web ブラウザで，IKE ポリシーの登録を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「VPN の設定」をクリックします．



VPN の設定画面で，VPN 動作モードに"ON"を選択し，IKE ポリシー(Phase 1 Policy)の登録を選択します.



IKE ポリシーの登録画面で，新規登録または，変更を行いたい番号を選択します.

新規登録画面



IKE ポリシーの登録画面で，各種設定を入力した後に「送信」をクリックします．.

登録変更画面



IKE ポリシーの登録画面で，各種設定を入力した後に「送信」をクリックします．.

【項目の説明】

VPN 識別：

この内容を ･････････････ 登録内容を修正する，または削除するかを選択します．
この項目は，登録変更画面のみ表示されます．

ポリシー識別子（1　16）･･ ポリシーエントリの識別子を設定します．

認証方法 ･･････････････ IKE の認証方式を Pre-Shared key または，RSA signatures から選択します．
Pre-Shared key を選択した場合は，次項の電子証明機能に関する設定を行わずに，5-11 の IPsec トンネルを確立する相手ルータ（ピアルータ）の登録から行ってください．

暗号化アルゴリズム ･････ 暗号化アルゴリズムを des または，3des から選択します．

Diffie-Hellman で使用する Oakley Group
････････････････････････ 鍵計算に使用する Diffie-Hellman Group を 1 または，2 から選択します．

ハッシュアルゴリズム ････ 認証アルゴリズムを MD5 または，SHA から選択します．

他の選択 ･･････････････ 他の登録内容を変更する場合，変更したい登録の番号を選択します．この項目は，登録変更画面のみ表示されます．

6.1.2　電子証明機能に関する設定

6.1.2.1　RSA signatures 機能で使用する鍵と電子証明書の登録

RSA signatures による認証方式では，鍵と電子証明書を使用します．

IKE Policy で RSA signatures を選択した場合，この章の手順に従い証明書を登録する必要があります．

鍵には秘密鍵と公開鍵の２種類があり，電子証明書についても自身の証明と CA センターの証明書があります．

本装置で RSA signatures 機能を使用するには，はじめに鍵を生成しその後電子証明書を取得，登録します．手順は以下の通りです．

鍵ペアの生成
パラメータの設定
リクエストの生成
証明書の入手
証明書の登録

6.1.2.1.1　Web ブラウザからの設定（鍵の生成と登録）

Web ブラウザで，RSA signatures 機能で使用する鍵の生成，登録を行います．



初期画面で「便利な設定」をクリックします．

⇩



ルータの便利な設定画面で「VPN の設定」をクリックします.



VPN の設定画面で，VPN 動作モードに"ON"を選択し，鍵ペアの生成を選択します.



鍵ペア生成画面で，"生成"ボタンをクリックして鍵ペアを生成します.



"生成"ボタンをクリック後，約３０秒ほどで"鍵ペア生成完了"のメッセージが表示され，鍵ペアの生成が完了しました.



鍵ペアの生成が完了したら，鍵を有効にするために装置のリセットを行います.

6.1.2.1.2 コンソールからの設定

コンソールまたは TELNET で本装置にログインし，RSA signatures 機能で使用する鍵の生成，登録を行います.

```
conf#vpngenkey size=1024                                        ①
generating a keypair…                                           ②
ok
conf#
```

①： 鍵の生成を行う際に，鍵のサイズを指定します.
サイズは，512bit～2048bit です.

②： 鍵の生成が行われています．ok の表示が出るまでしばらくお待ちください.
なお，サイズによる鍵の生成時間は以下の通りです.

512bit	約 3 秒
1024bit	約 30 秒
2048bit	約 3～8 分

鍵の生成が終了したら装置をリセットしてください.

メモ：既に鍵ペアが存在する場合は，②の箇所で Exist．New key pair create OK?(y/n)のメッセージが表示されますので，新しく鍵ペアを生成する場合は"y"を選択します.

以上で，鍵の登録が完了しました.
次に，証明書使用時のパラメータの設定を説明します.

6.1.2.1.3　Web ブラウザからの設定（証明書使用時のパラメータの設定）

Web ブラウザで，証明書使用時のパラメーターの設定を行います.



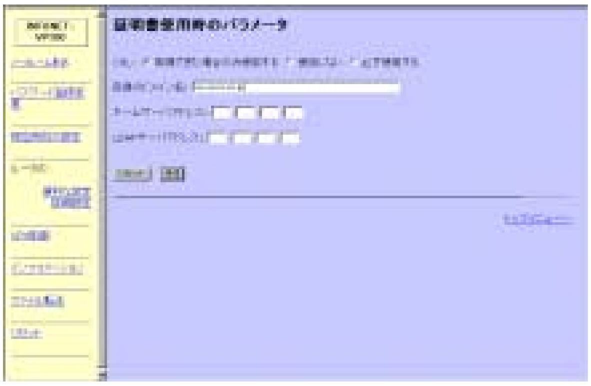
初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「VPN の設定」をクリックします.



VPN の設定画面で，VPN 動作モードに"ON"を選択し，証明書使用時のパラメータを選択します．



証明書使用時のパラメータ画面で，各種設定をおこないます．各種設定入力後に"送信"をクリックして登録します．
登録が終了すると，"証明書使用時のパラメータを以下の内容で登録しました．"と表示されます．
※登録が終了後，装置をリセットしてください．

【項目の説明】

CRL ······················ CRL を使用する/しない/取得できた場合のみ使用するから選択をします．

自身のドメイン名 ·········· 本装置が組み込まれている環境のドメイン名を設定します．

ネームサーバアドレス ······ 証明書に CRL の URL が含まれていて HTTP で CRL を取得する場合,URL から IP アドレスを求めるためにネームサーバを使用します．

LDAP サーバアドレス ········ CRL が LDAP サーバにおかれている場合設定します．

6.1.2.1.4　コンソールからの設定

コンソールまたは TELNET で本装置にログインし，証明書使用時のパラメータの設定を行います．

```
conf# vpncertparam domainname=www.xxx.co.jp                ①
conf#
```

①：　証明書使用時のパラメータとしてドメイン名を登録します．
　　　ドメイン名の登録が終了したら，装置をリセットしてください．

以上で，証明書使用時のパラメータの登録が完了しました．
次に，証明書リクエストの生成方法を説明します．

6.1.2.1.5 Web ブラウザからの設定(証明書リクエストの生成)

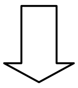
Web ブラウザで，証明書リクエストの生成を行います.



初期画面で「VPN 制御」をクリックします.



VPN 制御画面で，証明書リクエスト生成を選択します.





証明書リクエスト生成画面で，各種設定をおこないます．
設定が終了したら，生成をクリックします．

【項目の説明】

名前(CommonName) ………… 一般名を登録します．最大６４文字

組織(Organization) ……… 組織名を登録します．最大６４文字

国名(Country) …………… 国名を登録します．（２文字の国コード）

ドメイン名 ………………… ドメイン名を証明書リクエストに含めるかどうかを選択します．ドメイン名の設定については，P６-8を参照してください．

IPaddress ………………… IP アドレスを証明書にリクエストに含めるかどうかを選択します．含める IP アドレスは，PUBLIC LAN に割り当てられた IP アドレスです．



証明書のリクエストが終了すると，左のような画面になり，PEM 形式の証明書リクエストが表示されます．
PKCS#10 Base 64 (PEM)形式，PKCS#10 DER encoded 形式どちらかを選択して保存ボタンをクリックする事により，各形式で PC にファイルが保存されます．

本装置で作成した証明書のリクエスト使用して，CA センターから証明書を取得します．
CA センターでの証明書の取得方法は，各 CA センターの指示に従って行ってください．

6.1.2.1.6　コンソールからの設定

コンソールまたはTELNETで本装置にログインし，証明書リクエストの生成を行います．

```
conf#vpncertreq CN=XXX O=YYY C=jp domainname ip                        ①
-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwLTELMAkGA1UEBhMCanAxDzANBgNVBAoTBmRlbmtvdTENMAsG
A1UEAxMEZnVydTCBnTANBgkqhkiG9w0BAQEFAAOBiwAwgYcCgYEAiUXsnMDkEK0B
V4I78L/XjCjhMF+U49AinRrvBt2jPxTmlwlXH2AnnKPoFjXOY9MBv1aeTrdKXlNL
H3Ysan4HmcKQAR/iSSGybKrq809GSBmqGiKzv2PyZX45PXwIqSuui+Q7jHQBZC0F
thfXeL69etZK3SIeaP3zQWlACTkMSHcCASGgQjBABgkqhkiG9w0BCQ4xMzAxMAsG
A1UdDwQEAwIFoDAiBgNVHREEGzAZghdqYWNrbWlnaS5mdXJ1a2F3YS5jby5qcDAN
BgkqhkiG9w0BAQUFAAOBgQBRsKfc7Bwh0nQL5YsxSfNCBm+ujvxpy1ASYvnEL54K
BeYMKvCop/PgIESGL3XJ+Au30VXVCJ6gM3zQkXKYj0AuvRyS+IQ3pa1L1aSbb4xm
HMjL5wOdmzuhHbok870i4y/T2/FdBAyV0sxNQxAGSejG7QzuqwSBfa62UMRQgCmq
tg==
-----END CERTIFICATE REQUEST-----
conf#
```

①：　証明書リクエストの生成に必要な，名前（CN），組織（O），国名（C）を設定します．また，ドメイン名，IPアドレスを含める場合は，上例のように"domain name"，"ip"を指定します．
入力が終了すると，画面のようにPEM形式の証明書リクエストが表示されます．

本装置で作成した証明書のリクエスト使用して，CAセンターから証明書を取得します．
CAセンターでの証明書の取得方法は，各CAセンターの指示に従って行ってください．

以上で，証明書リクエストの生成が完了しました．
次に，取得した証明書の登録方法を説明します．

6.1.2.1.7　Web ブラウザからの設定（証明書の登録）

Web ブラウザで，RSA signatures 機能で使用する証明書の登録を行います．
証明書の登録には，自身の証明書と，CA の証明書共に登録する必要があります．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「VPN の設定」をクリックします．



VPN の設定画面で，VPN 動作モードに"ON"を選択し，証明書の登録を選択します．



証明書の登録画面で，新しく証明書を登録する場合は，新規登録をクリックします．
既に，登録してある証明書を削除する場合は，対象とする番号を入力して送信をクリックする事により削除ができます．



証明書の登録画面で，各種設定をおこないます．
画面中央のウィンドウに自身または **CA** センターで取得した証明書をペーストします．
設定が終了したら，登録をクリックします．
証明書の登録は即時有効なので，リセットの必要はありません．

【項目の説明】

信頼できる root CA の証明書である
･･････････････････････････ CA からの証明書を登録する場合はチェックします．自身の証明書を登録する場合は，チェックをしないでください．

PEM format ････････････････ PEM format の証明書をペースとして登録する場合選択してください．

ファイル ･･････････････････ PC に保存してある証明書を参照して登録する場合に選択します．

6.1.2.1.8　コンソールからの設定

コンソールまたは TELNET で本装置にログインし，証明書の登録を行います．

```
conf#vpncert add                                                ①
"Input certificate"
```

①： vpncert add と入力すると"Input certificate" と表示されるので，CA センターで取得した証明書を登録します．

証明書の登録は即時有効なので，リセットの必要はありません．

CA センター証明書を登録する場合は，”vpncert add root ”と入力します．

```
conf#vpncert add root                                           ①
"Input certificate"
```

証明書を追加する場合，証明書の入力が終了した後^d（Control+d）を入力します．

6.2 IPsec トンネルを確立する相手ルータ（ピアルータ）の登録

IPsec 機能を使用する場合は，論理的な IPsec トンネルを確立する必要があり，IPsec トンネルを確立する相手ルータを登録しておく必要があります．本書では，IPsec トンネルを確立する相手ルータをピアルータと記述する場合もあります．

6.2.1 Web ブラウザからの設定

Web ブラウザで，IPsec トンネルを確立するピアルータの登録を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「VPN の設定」をクリックします．



VPN の設定画面で，VPN 動作モードに"ON"を選択し，VPN ピアの登録を選択します.



VPN ピアの登録画面で，変更をおこないたい番号を選択します.

※登録データが無い場合は登録リストは表示されません.



VPN ピアの登録画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

VPN 識別：

IP アドレス ･････････････ VPN ピアの IP アドレスを設定します.

名称指定 ････････････････ VPN ピアの名前を設定します.
VPN ピアが Dial-up 接続して IP アドレスを取得する場合等で, IP アドレスが固定では無い場合, IP アドレスではなく名前で指定できます. RSA signatures の場合は, VPN ピアの ID を（名前やドメイン名）を指定します.

こちらの名前 ････････････ 本装置側の名前を設定します.
将来拡張用のため, 特に設定する必要はありません.

こちらのパスワード ･･････ 本装置側のパスワードを設定します.
将来拡張用のため, 特に設定する必要はありません.

鍵データ：

文字列 ･･････････････････ VPN ピアに依存する鍵データを ASCII データで設定します.

バイナリ（16 進） ･･･････ VPN ピアに依存する鍵データをバイナリ（16 進数）データで設定します.

NAT 動作モード ･･････････ VPN ピア毎の NAT 動作モードを指定します.

off ･････････････････････ NAT 変換しません.

nat ･････････････････････ NAT のモード, 変換アドレス等, 装置としての NAT の設定に従います.

nat+ ････････････････････ NAT+モードとして動作します.

peer nat ････････････････ 指定したアドレスを使用して NAT+モードとして動作します.

自身の ID ･･･････････････ 自身の ID を「domainname」「IPaddress」から選択します.

ポリシー識別子による登録済み IKE ポリシーの指定
･････････････････ 設定している相手と接続する際の IKE ポリシーを選択します.

6.2.2　コンソールからの設定

コンソールまたは TELNET で本装置にログインし，IPsec トンネルを確立するピアルータの登録を行います．設定はコンフィグレーションモードで行います．

```
conf#vpn on                                              ①
conf#vpnpeer add addr=1.1.1.1 key=secret                 ②
```

①： VPN 機能を使用するために，使用するかどうかの設定を on にします．

②： VPN 機能を使用して確立したトンネルで接続する相手装置の IP アドレスを入力します．つづいて，VPN キーの入力をします．

6.3 暗号化方式の登録

IPsec トンネルを確立する際に，相手ルータとの暗号化方式を登録しておく必要があります.

6.3.1 Web ブラウザからの設定

Web ブラウザで，暗号化ポリシーの登録を行います.



初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「VPN の設定」をクリックします.



VPN の設定画面で，VPN 動作モードに"ON"を選択し，暗号化ポリシーの登録を選択します.



暗号化ポリシーの登録画面で，新規登録を選択します.

既に登録してある設定を変更する場合は，対象とする設定番号を選択してください.



暗号化ポリシーの登録画面で，各種設定を入力した後に「送信」をクリックします．.

【項目の説明】

ポリシー識別子 ············ 暗号化ポリシーエントリの識別子.

SA ライフタイム：

デフォルトを使用する ···· 通常はこちらを選択してください.

設定値を使用する ········ 変更する場合は，VPN ピアどうしで同じ値になるように設定してください.

鍵データ（PFS）の再生成：

再生成する ·············· SA 確立時に新たな鍵情報を指定します.

再生成しない ············ 鍵情報を再生成しない.

暗号化アルゴリズム ········ null，des，3des のどちらかを選択します.

認証アルゴリズム ·········· null，hmac-md5，hmac-sha のどれかを選択します.

6.3.2 コンソールからの設定

コンソールまたは TELNET で本装置にログインし，IPsec トンネルを確立する際に，相手ルータとの暗号化方式を登録しておく必要があります．設定はコンフィグレーションモードで行います.

```
conf#vpnpolicy add id=1                                        ①
```

①： ポリシー識別子を入力します.

６．４ VPN対象パケットの登録

VPNの対象とするパケットの登録方法を以下に示します.

６．４．１　Webブラウザからの設定

Webブラウザで，VPNの対象とするパケットの登録を行います.



初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「VPN の設定」をクリックします.



VPN の設定画面で，VPN 動作モードに"ON"を選択し，VPN対象パケットの登録を選択します.



VPN 対象のパケットの登録画面で，新規登録を選択します．
既に登録してある設定を変更する場合は，対象とする設定番号を選択してください．

※登録データが無い場合は登録リストは表示されません．



VPN 対象パケットの登録画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

パケット優先順位 ･･････････ VPN 対象データのエントリの識別子．

宛先指定：

全て ････････････････････ 全てのパケットを対象とします．

宛先が VPN ピアの時 ･･････ VPN ピアに登録してある IP アドレスを対象とします．

IP アドレス指定 ･････････ 対象とするパケットの IP アドレス，アドレスマスクを指定

します.

宛先ポート指定 ………… 全てのポートまたは，ポートを指定します.

送信元指定：

全て………………… 全てのパケットを対象とします.

IP アドレス指定 ……… 対象とするパケットの IP アドレス，アドレスマスクを指定します.

送信元ポート指定 ……… 全てのポートまたは，ポートを指定します.

プロトコル指定 ………… icmp，tcp，udp または全てのいずれかを選択します.

任意指定時はプロトコル番号を設定

……………………… 該当するプロトコル番号を指定します.

IPsec 処理タイプ：

IPsec 処理して中継 …… IPsec による VPN 通信を行います.

IPsec 処理しないで中継 ‥ VPN 通信を行わず，通常の通信を行います.

廃棄………………… 該当しないパケットは廃棄します.

以下の設定は「IPsec 処理タイプ」に「IPsec 処理して中継」を選択した時に有効となります.

SA 確立契機…………… SA 確立契機を起動時に行うかどうかの指定後, データ通信時, ライフタイム満了時，指定時刻時の指定をおこないます.

登録済み VPN ピア指定 …… 登録済み VPN ピアから IP アドレス，または名称で指定します.

ポリシー識別子による登録済み暗号化ポリシーの指定

……………………… 登録してある暗号化ポリシーの中から指定します.

6.4.2 コンソールからの設定

コンソールまたはTELNETで本装置にログインし，VPNの対象とするパケットの登録を行います．設定はコンフィグレーションモードで行います．

```
conf#vpnselector add id=1 dst=192.52.128.0,255.255.255.0      ①
src=192.168.56.0,255.255.255.0 peeraddr=192.168.55.1 policy=1
```

①： パケット優先順位，対象とするパケットの送信元／先のIPアドレス，相手装置のIPアドレス，暗号化ポリシーの指定を行います．

7 NAT（アドレス変換）機能

NAT（Network Address Translation）機能とは，PRIVATE LANで使用しているIPアドレスを，別のIPアドレスに変換して，PUBLIC LANに接続する機能です．本装置の変換テーブルは，256（NAT），512（NAT+）エントリです．

NAT機能を使用するメリットは，大きく分けて以下の2種類があります．

（1） PRIVATE LANで使用しているローカルIPアドレス※1を，グローバルIPアドレス※2に変換する．

（2） PRIVATE LANで使用しているIPアドレスを，セキュリティ上外部に広告しないようにするため，別のIPアドレスに変換する．

さらに，NAPT機能を使用することにより，複数の端末のIPアドレスを一つのIPアドレスに集約することができるので，PUBLIC LAN側に一つのIPアドレスしか割り当てられない場合でも，複数台の端末のアドレス変換を行うことができます．

※１： ローカルIPアドレス
インターネット等のグローバルなTCP/IP環境では，使用してはいけないIPアドレス．インターネットには接続しないLAN環境等で利用されることが多い．

※２： グローバルIPアドレス
JPNICから正式に割り当てられたIPアドレス，または契約したプロバイダ等から割り当てられたIPアドレス．グローバルなTCP/IP環境に接続することが許可されたIPアドレス．IPsecトンネルを確立する相手ルータ（ピアルータ）の登録パブリック

７．１ NATスタティックの登録

NATスタティックの登録方法を以下に示します．
エントリ数は128件です．

７．１．１ Webブラウザからの設定

Webブラウザで，NATスタティックの登録を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「NAT$^+$機能」をクリックします.



NAT$^+$機能の設定画面で，NAT$^+$機能に"ON"を選択し，NAT スタティックの登録を選択します.



NAT スタティック登録画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

PRIVATE LAN 上の端末指定 IP アドレス
･････････････････････････ PRIVATE LAN 側に接続されている，変更対象とする装置の IP アドレスを設定します．

PUBLIC LAN に見える IP アドレス
･････････････････････････ 変更後の PUBLIC LAN の IP アドレスを設定します．

7.1.2　コンソールからの設定

コンソールまたは TELNET で本装置にログインし，NAT スタティックの登録を行います．設定はコンフィグレーションモードで行います．

```
conf#nat nat                                                  ①
conf#natstatictable add local=192.168.100.1 global=1.1.1.1    ②
```

①： NAT 機能を使用するために，使用するかどうかの設定を on にします．

②： NAT スタティックテーブルに，変換対象とするローカルアドレスと，変換後のグローバルアドレスを設定します．

7.2 NAT+スタティックの登録

NAT+スタティックの登録方法を以下に示します.

エントリ数は 16 件です.

7.2.1 Web ブラウザからの設定

Web ブラウザで，NAT+スタティックの登録を行います.



初期画面で「便利な設定」をクリックします.

⇩



ルータの便利な設定画面で「NAT+機能」をクリックします.

⇩



NAT+機能の画面で，NAT+機能に"ON"を選択し，NAT+スタティックの登録を選択します．



NAT+スタティックの画面で，新規登録を選択します．既に登録してある設定を変更する場合は，対象とする設定番号を選択してください．



NAT+スタティック登録画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

PRIVATE LAN 上の端末指定：

IP アドレス ・・・・・・・・・・・・ PRIVATE LAN 側に接続されている，NAT+変換対象とする装置の IP アドレスを設定します．

ポート番号 ・・・・・・・・・・・・・ NAT+変換するパケットの送信元ポート番号を設定します．

PUBLIC LAN に見える IP アドレスとポート番号：

IP アドレス ･･････････････ PUBLIC LAN 側に見える，NAT+変換後の IP アドレスを設定します．

ポート番号 ･･････････････ NAT+変換後のポート番号を設定します．

7.2.2 コンソールからの設定

コンソールまたは TELNET で本装置にログインし，NAT+スタティックの登録を行います．設定はコンフィグレーションモードで行います．

```
conf#nat natp                                                        ①
conf#natplusstatictable add virtual=192.168.100.1,1025
local=1.1.1.1,2000                                                   ②
```

①： NAT+機能を使用するために，使用するかどうかの設定を on にします．

②： NAT+スタティックテーブルに，NAT+変換対象とする IP アドレスとポート番号，変換後の IP アドレスとポート番号を設定します．

7.3 NATの拡張設定

natnotrans，natrangeの設定方法を以下に示します.

上記のコマンドはWEB設定からは行えません.

7.3.1 natnotransの設定

NAT変換しないPRIVATE LAN側のIPアドレスを設定します.

ここで設定しないIPアドレスは「変換後のアドレス範囲」にしたがってNAT変換されます.

```
conf#natnotrans add private=xxx.xxx.xxx.1,255.255.255.255        ①
```

①： NAT変換しないIPアドレスと，マスクを設定します.

【項目の説明】

private‥‥‥‥‥‥‥‥‥ PRIVATE LAN 側に接続されている，NAT+変換対象としない装置のIPアドレスを設定します.

7.3.2 natrangeの設定

NAT変換するPUBLIC LAN側のIPアドレスの範囲を設定します.

natrangeの設定は，NAT+では行えません.

```
conf#natrange add begin=xxx.xxx.xxx.1 end= xxx.xxx.xxx.255        ①
```

①： NAT変換する範囲の先頭のIPアドレスと，最後のIPアドレスを設定します.

【項目の説明】

begin‥‥‥‥‥‥‥‥‥‥ NAT変換するPUBLIC LAN側の先頭のIPアドレスを設定します.

end‥‥‥‥‥‥‥‥‥‥‥ NAT変換するPUBLIC LAN側の最後のIPアドレスを設定します.

本装置でNAT機能を使用する場合は，スタティックルーティングの設定（5-11）を行う必要があります.
NAT変換対象アドレスを宛先アドレスに指定し，PRIVATE LANに設定したIPアドレスをゲートウェイアドレスに指定したスタティックテーブルを設定します.

8 DHCP サーバ機能

DHCP サーバ機能とは，PRIVATE LAN 側に接続されている端末に対して，自動的に IP アドレスを割り当てることのできる機能です．

また，DHCP スタティックに登録する事により，任意の IP アドレスを割り当てることもできます．

本装置の対応端末数は 254 台です．また，DHCP スタティックは 16 エントリです．

8.1 DHCP サーバ機能の設定

DHCP サーバ機能の設定方法を以下に示します．

8.1.1 Web ブラウザからの設定

Web ブラウザで，DHCP サーバ機能の設定を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「DHCP サーバ機能」をクリックします．



DHCP サーバ機能設定画面で, 各種設定を入力した後に「送信」をクリックします. .

【項目の説明】

DHCP サーバ機能･･･････････ DHCP サーバ機能を使用する場合は on に設定します.

配付 IP アドレスの開始値 ･･･ DHCP 機能を使用して, 自動的に割り当てる IP アドレスの開始値を指定します.

デフォルトゲートウエイの通知
････････････････････････ デフォルトゲートウェイの IP アドレスを通知するかどうかの指定をします.

ドメイン名称の通知 ･･･････ ドメイン名称を通知するかどうかを設定します.
　通知するドメイン名称 ････ 通知するドメイン名称を登録します.

DNS アドレスの通知･･････････ DNS サーバの IP アドレスを通知するかどうかを設定します.
　DNS プライマリアドレス･･･ DNS プライマリサーバのアドレスを登録します.
　DNS セカンダリアドレス･･･ DNS セカンダリサーバのアドレスを登録します.

WINS アドレスの通知･･･････ WINS サーバの IP アドレスを通知するかどうかを設定します.
　WINS プライマリアドレス･･ WINS プライマリサーバのアドレスを登録します.
　WINS セカンダリアドレス･･ WINS セカンダリサーバのアドレスを登録します.

配付アドレスのスタティック登録
････････････････････････ 任意の IP アドレスを割り当てたい場合は, 対象とする装置

の MAC アドレスと割り当てたい IP アドレスの組み合わせを登録します.

8.1.2 コンソールからの設定

コンソールまたは TELNET で本装置にログインし，DHCP サーバの設定を行います．設定はコンフィグレーションモードで行います.

```
conf#dhcpserver on gateway=on                                    ①
conf#hostname nameserver=192.168.100.1 domainname=VP100.co.jp   ②
```

①： DHCP サーバ機能を使用する場合，設定を on にします.
デフォルトゲートウェイの通知を行います.

②： DNS アドレスを 192.168.100.1 として通知します.
ドメインネームを VP100.co.jp として通知します.

9 syslog 機能

syslog 機能を使用する事により，tlog，elog，llog，vlog，vpnlog，clog，flog の各種ログを指定した端末に送信する事ができます．

9.1 syslog 機能の設定

syslog 機能の設定方法を以下に示します．

9.1.1 Web ブラウザからの設定

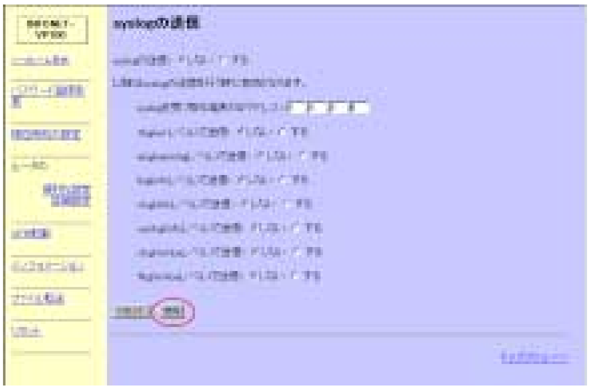
Web ブラウザで，syslog 機能の設定を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「syslog 機能」をクリックします．



syslog の送信画面で，各種設定を入力した後に「送信」をクリックします．．

【項目の説明】

syslog の送信・・・・・・・・・・・・・ syslog の送信を行う場合は on に設定します．

syslog を受け取る端末の IP アドレス
・・・・・・・・・・・・・・・・・・・・・・・・・ syslog を受け取る端末の IP アドレスを設定します．

tlog(err レベル)で送信・・・・・ tlog 情報を送信するかどうかの設定．

elog(warning レベル)で送信・ elog 情報を送信するかどうかの設定．

llog(info レベル)で送信・・・・ llog 情報を送信するかどうかの設定．

vlog(info レベル)で送信・・・・ vlog 情報を送信するかどうかの設定．

vpnlog(info レベル)で送信・・ vpnlog 情報を送信するかどうかの設定．

clog（notice レベル）で送信
・・・・・・・・・・・・・・・・・・・ clog 情報を送信するかどうかの設定．

flog（notice レベル）で送信
・・・・・・・・・・・・・・・・・・・ flog 情報を送信するかどうかの設定．

9.1.2 コンソールからの設定

コンソールまたは TELNET で本装置にログインし，syslog 機能の設定を行います．設定はコンフィグレーションモードで行います．

```
conf#syslogcontrol on                                                    ①
conf#syslogtable addr=192.168.100.1 err=tlog warning=elog
info=llog,vlog,vpnlog notice=clog,flog facility=0                        ②
```

①： syslog 機能を使用する場合，設定を on にします．

②：192.168.100.1 の端末宛に,err レベルとして tlog／warning レベルとして elog／info レベルとして llog,vlog,vpnlog／notice レベルとして clog，flog，ファシリティーを０とします．

10 SNMP エージェント機能

コンソールまたは TELNET で本装置にログインし，SNMP エージェント機能の設定を行います．設定はコンフィグレーションモードで行います．SNMP エージェント機能の設定は，コマンドラインのみです．snmp コマンドと manager コマンドで設定します．

snmp [on|off] [authtrap[={on|off}]]

パラメータ

on|off ・・・・・・・・・・・・・・・・・・ 本装置を SNMP エージェントとして使用する／しないを指定します．
設定範囲：on，off
工場出荷時：on

authtrap[={on|off}] ・・・・・ 認証失敗時，トラップを受け付けるマネージャに対して認証失敗トラップを送信する／しないを指定します．
設定範囲：on，off
工場出荷時：on

manager △[[add△<index>
△[addr=ipaddress]△name=<community name>
△[mode={trw|rw|tr|r}]]
|[delete△{<index>|all}]]

パラメータ

add△<index>|[delete△{<index>|all}]
・・・・・・・・・・・・・・・・・・・・・・・・ 指定のテーブルを登録および削除します．テーブルは最大 4 件登録できます．

addr=ipaddress ・・・・・・・・・・ SNMP マネージャの IP アドレスを指定します．「0.0.0.0」はデフォルトマネージャ（すべての装置が本装置の SNMP エージェント機能を使用可能）のエントリを示します．省略時は，0.0.0.0 となります．
設定範囲：0.0.0.0 255.255.255.255
工場出荷時：0.0.0.0

name=<community△name> ・・ SNMP マネージャと通信する場合のコミュニティ名を英数字 32 文字以内で指定します．
設定範囲：最大 32 文字の英数字
工場出荷時：public

mode={trw|rw|tr|r}・・・・・・ マネージャの動作モードを指定します.省略時は r となります.
設定範囲：trw，rw，tr，r
t:トラップ送信
r:GET 可能
w:SET 可能
工場出荷時：r

SNMP エージェント機能の設定方法を以下に示します.

```
conf#snmp on authtrap=on                                       ①
conf#manager add 1 addr=192.168.100.1 name=public mode=trw    ②
```

①： SNMP エージェント機能を使用する場合，設定を on にします.
トラップ送信を行う場合は，設定を on にします.
②： SNMP マネージャのアドレス，コミュニティー名，動作モードを設定します.

11 バックアップ機能

本装置では，同一ネットワーク上の複数のINFONET-VP100がある場合，１つのINFONET-VP100に故障が発生した場合でも，端末等の設定をまったく変更せずに，他のINFONET-VP100が代替機となりバックアップを行うことができます．バックアップ機能を使用する場合，複数のINFONET-VP100で論理的なグループを形成する必要があります．本装置では，論理的なグループを形成することをルータグループ機能と呼びます．

１１.１グループ化の設定

バックアップ機能を使用するためのルータグループ機能の設定方法を以下に示します．

１１.１.１　　Webブラウザからの設定

Webブラウザで，ルータグループ機能の設定を行います．



初期画面で「便利な設定」をクリックします．



ルータの便利な設定画面で「ルータグループ機能」をクリックします．



ルータグループ機能の各種設定を入力した後に「送信」をクリックします.

【項目の説明】

id ・・・・・・・・・・・・・・・・・・・・・・・・ ルータグループ ID を指定します. ルータグループを形成するルータ同士では, 同じ値である必要があります.

Send Interval ・・・・・・・・・・・・・ Master ルータが送信する VRRP 公告パケットの送信間隔(秒)を設定します.

Owner/Not owner ・・・・・・・・・・・ Mater ルータとして動作する場合に, そのグループの仮想 IP アドレスを自分の実 IP アドレスと同じとする場合に, Owner の設定をします. 通常, バックアップルータを追加する場合に, 先に設置しているルータの RGRP を ON にする場合に, この設定を利用します.

IP address ・・・・・・・・・・・・・・・・ ルータグループの仮想 IP アドレスを指定します. Owner の場合は, 指定する必要がありません. 自分が Master ルータの場合であっても, 通常, 実 IP アドレスと違うアドレスをグループの仮想 IP アドレスとして指定します.

Priority ・・・・・・・・・・・・・・・・・・ ルータの優先度を設定します. 大きい数字ほど優先度は高くなります. この優先度は, Master ルータに障害が発生した場合に作動する順番に使用されます.

preempt ・・・・・・・・・・・・・・・・・・・ 他に Master ルータがいる状態で, 自分に設定された Priority の方が高い場合, 自分を Master ルータとして公告を開始するかどうかを設定します.

１１.１.２　　コンソールからの設定

コンソールまたはTELNETで本装置にログインし，ルータグループ機能の設定を行います．設定はコンフィグレーションモードで行います．

```
conf#rgrpparam on                                              ①
conf#rgrptable add id=1 addr=192.168.0.1,172.xxx.xxx.1         ②
```

①： ルータグループ機能を使用する場合，設定をonにします．

②： 自分を id=1 のグループの Master ルータとして動作させます．バックアップルータとして動作させる場合は，”addr=”でMasterルータのIPアドレスを設定します。

【バックアップ機能使用時の注意／制限事項】

・VPN機能で,RSAsignaturesを使用している場合は,バックアップ機能が使用できません．pre-sharedキーの場合は，バックアップ機能が使用できます．→P６-1参照

・トランスペアレントモードとの併用はできません．

・RIPは使用できません．LAN上の端末・ルータは，ゲートウェイのアドレスが仮想IPアドレスであるデフォルトゲートウェイあるいはスタティックルーティングを設定してください．

・natの設定でnat+とし（P７-1），vpnpeerの設定でNATモードをnat（P６-17）にした場合,バックアップ機能を使用することができません.この場合はNATモードをpeernatに設定し，アドレスに変換するアドレスを入力することで実現できます．

・DHCPサーバ機能を使用する場合，デフォルトゲートウェイの通知はoffを選択し（P８-1），各端末でデフォルトゲートウェイの設定にMasterルータのIPアドレスを指定してください。

・INFONET-VP100がResponderとして確立されているSAでは,バックアップ機能が作動した場合，Initiator側がlifetime間SAを開放しませんので，その間通信ができなくなります．

12ログ取得機能

本装置では，以下のログを取得することができます.

エラーログ（elog） ･････････････････････ 装置の中・軽度の障害情報を表示します.
ラインログ（llog） ･････････････････････ PRIVATE/PUBLIC LAN の情報を表示します.
トラップログ（tlog） ･･･････････････････ 装置の重度障害情報を表示します.
イベントログ（vlog） ･･･････････････････ FTP/TELNET など装置へのアクセス情報を表示します.
VPN 関連ログ（vpnlog） ･････････････････ VPN 関連のログを表示します.
通信パケットログ（clog） ･･･････････････ 設定した内容のパケット数情報を表示します.
IP パケットフィルター廃棄ログ（flog） ･ フィルタリング機能によりフィルタされたパケットの情報を表示します.

VPN 関連ログ, 通信パケットログ, IP パケットフィルター廃棄ログは, ログを取得するかどうか, また，通信パケットログの場合は取得するパケットの情報を設定する必要があります．本章では, 上記のログを表示するための設定方法について説明します.

１２.１　VPN 関連ログ

VPN 関連ログでは，VPN 関連ログに SA の確立情報を載せるかどうかを設定します．この設定は, Web ブラウザもしくはコマンドで設定します.

１２.１.１　　Web ブラウザからの設定

Web ブラウザで，VPN 関連ログに SA の確立情報を載せるかどうかの設定方法を示します.



初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「VPN の設定」をクリックします.



VPN の設定画面で，VPN 動作モードに"ON"を選択し，VPN ログモードの登録を選択します.



SA 確立の情報を VPN ログに残すかどうかを選択し，「送信」ボタンをクリックします.

12.1.2　コンソールからの設定

コンソールまたは TELNET で本装置にログインし，VPN 関連ログに SA の確立情報を載せるかどうかの設定を行います．設定はコンフィグレーションモードで行います.

```
conf#vpnopt vpnlog=on
```

１２.２　通信パケットログ

通信パケットログでは，以下の種類のパケット情報を表示することができます.

【INFONET-VP100 が中継したパケット】

【INFONET-VP100 が送受信したパケット】

上記のそれぞれの種類について，表示する／しないを設定します.　この設定は，Web ブラウザもしくはコマンドで設定します.

１２.２.１　　Web ブラウザからの設定

Web ブラウザで，通信パケットログの設定をします.



初期画面で「便利な設定」をクリックします.



ルータの便利な設定画面で「IP 通信パケットログ」をクリックします.



clog の記録で"する"を選択し，「送信」をクリックします．．

その後，「中継したパケットのログを取る」または「VP100 が送受信した IP パケットのログを取る」をクリックし，記録する通信パケットを設定します.

中継したパケットのログを取るをクリックした場合



記録したいパケットをクリックし，「送信」ボタンをクリックします.

12.2.2　　コンソールからの設定

コンソールまたは TELNET で本装置にログインし, 通信パケットログを記録するかどうかおよび通信パケットの種類を設定します．設定はコンフィグレーションモードで行います.

以下は，INFONET-VP100 からパブリック LAN に送信するパケットを記録する例です.

```
conf#clogcontrol on
conf#clogcontrol add prot=all type=send,public
```

12.3　IP パケットフィルター廃棄ログ

IP パケットフィルタリング機能により廃棄されたログを記録するかどうかを設定します．この設定は，コマンドでのみ行うことができます．設定はコンフィグレーションモードで行います.

```
conf#flogcontrol on
```

13インフォメーション

インフォメーションを選択することにより，装置の各種情報を確認することができます.
確認できる項目は以下の通りです.

装置について
統計情報の表示
ルーティングインタフェースの表示
ルーティング状態の表示
DHCPの状態表示
NAT+の状態表示
IKE SAの状態表示
IPSEC SAの状態表示
証明書表示
証明書取消リスト(CRL)表示
エラーログの表示
回線ログの表示
イベントログの表示
VPNログの表示
通信パケットログの表示
IPパケットフィルター廃棄ログの表示

１３.１装置について

端末情報を表示します．

１３.１.１　　Web ブラウザからの操作

Web ブラウザで，端末情報を表示する方法を示します．



初期画面で「インフォメーション」をクリックします．

⇩



インフォメーション画面で「装置について」をクリックします．

⇩



装置 ID，装置現在時刻が表示されます．

【項目の説明】

装置 ID の表示 ･････････････ 装置名称，ファームウェア版数，装置の MAC アドレスが表示されます．

装置現在時刻 ･･････････････ 装置に設定されている現在時刻が表示されます．

13.1.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，端末情報の表示方法を説明します．操作はコンフィグレーションモードで行います．

装置については hereis コマンドと date コマンドで表示させることができます．

```
#hereis
description: 'INFONET-VP100' A V01.00 1999.12.03 (00:00:0e:87:c0:0f)
node         :VP100
manager      :root
location     :Tokyo

#date
000817.105812 (0 17:56:36)
```

【項目の説明】

description･････････････ 装置名称，ファームウェア版数，装置の MAC アドレスが表示されます．

node････････････････････ 装置名称が表示されます．

manager･････････････････ 管理者名が表示されます．

location････････････････ 装置設置場所が表示されます．

date････････････････････ 装置現在時刻が表示されます．

１３．２システムの状態表示

システム情報を表示します．

１３．２．１　　Web ブラウザからの操作

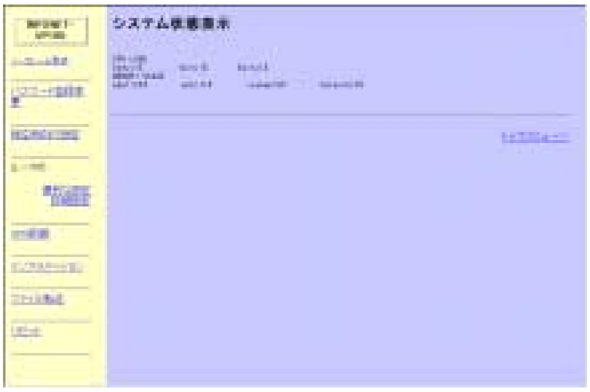
Web ブラウザで，統計情報を表示する方法を示します．



初期画面で「インフォメーション」をクリックします．



インフォメーション画面で「システムの状態表示」をクリックします．



システム情報が表示されます.

【項目の説明】

CPU LOAD：

- 5sec・・・・・・・・・・・・・・・・ 最新の５秒間の平均CPU負荷率（%）
- 1min・・・・・・・・・・・・・・・・ 最新の１分間の平均CPU負荷率（%）
- 5min・・・・・・・・・・・・・・・・ 最新の５分間の平均CPU負荷率（%）

CPU LOAD：

- mbuf・・・・・・・・・・・・・・・・ mbuf使用率（%）
- mcb・・・・・・・・・・・・・・・・・ mcb使用率（%）
- isakmp・・・・・・・・・・・・・・ isakmpメモリ使用率（%）
- network・・・・・・・・・・・・・ networkメモリ使用率（%）

１３.２.２　　コンソールからの操作

コンソールまたはTELNETで本装置にログインし，システム情報の表示方法を説明します．操作はノーマルモードで行います．

システム情報は，stsystemコマンドで表示させることができます．

```
#stsystem
CPU LOAD
5sec:12%        1min:1%        5min:1%
MEMORY USAGE
mbuf:13%        mcb:0%         isakmp:0%        network:0%
#
```

１３.３統計情報の表示

統計情報を表示します.

１３.３.１　　Web ブラウザからの操作

Web ブラウザで，統計情報を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「統計情報の表示」をクリックします.



装置の統計情報が表示されます.

【項目の説明】

回線統計情報：

alignment error frames
・・・・・・・・・・・・・・・・・・・ フレーム長がオクテット整数でなく，FCS チェックにもエラーした受信フレームの総数

FCS error frames ・・・・ フレーム長はオクテット整数だがFCSエラーで廃棄された受信フレーム総数

collision count ・・・・・ コリジョン発生回数

ルーティング統計情報：

<IP>
in packet・・・・・・・・・・・ 総入力 IP パケット数
in discard packet・・・ 廃棄された入力パケット数
in header errors packet
・・・・・・・・・・・・・・・・・・・・ IP ヘッダエラー受信パケット数
in address error packet
・・・・・・・・・・・・・・・・・・・・ IP アドレスエラー受信パケット数
out request packet・・ 送信要求パケット数
out discard packet・・ 内部資源不足のため廃棄された送信要求パケット数
forward packet・・・・・・ フォワーディングの必要のある受信パケット数
no route packet・・・・・ 送信経路がないため廃棄された送信要求パケット数

<ICMP>
in message packet・・・ 受信 ICMP パケット数（エラー含む）
in error packet・・・・・ 受信 ICMP エラーパケット数
out message packet・・ 送信 ICMP パケット数（エラー含む）
out error packet・・・・ 送信 ICMP エラーパケット数

<UDP>
in datagram packet・・ 受信 UDP データグラム数
in error packet・・・・・ 受信エラーUDP データグラム数（チェックサムエラー等）
no port packet・・・・・・ 受信エラーUDP データグラム数（不正宛先ポート）
out datagram packet・ 送信 UDP データグラム数

<TCP>
in segment packet・・・ 受信 TCP セグメント数
out segment packet・・ 送信 TCP セグメント数
in error packet・・・・・ 受信エラーTCP セグメント数（チェックサムエラー等）
passive open count・・ 受動オープンした回数

<RIP>
in packet・・・・・・・・・・・ 受信 RIP パケット数
sent packet・・・・・・・・・ 送信 RIP パケット数
out request packet・・ 送信 RIP 要求パケット数
in reply packet・・・・・ 受信 RIP リプライパケット数
flash update packet・ 「triggered update」した回数
send error packet・・・ 送信エラーパケット数
bad receive packet・・ 受信エラーパケット数

VPN統計情報：
PI send packet･･････････ Phase I 送信パケット数
PI receive packet･･････ Phase I 受信パケット数
PI discard packet･･････ Phase I 廃棄パケット数
PI decrypt error packet･ Phase I 復号化エラーパケット数
PI hash error packet･･･ Phase I ハッシュエラーパケット数
PI exchange fail･･･････ IKE SA 確立エラー数
PI exchange success････ IKE SA 確立数

xauth send packet･･････ 拡張認証 送信パケット数
xauth receive packet･･･ 拡張認証 受信パケット数
xauth discard packet･･･ 拡張認証 廃棄パケット数
xauth exchange error･･･ 拡張認証 失敗数
xauth exchange success･･ 拡張認証 成功数

PII send packet･････････ Phase II 送信パケット数
PII receive packet･････ Phase II 受信パケット数
PII discard packet･････ Phase II 廃棄パケット数
PII decrypt error packet Phase II 復号化エラーパケット数
PII hash error packet･･･ Phase II ハッシュエラーパケット数
PII exchange fail･･････ IPsec SA 確立エラー数
PII exchange success･･･ IPsec SA 確立数

notify send packet･････ Notifyメッセージ送信数
notify receive packet･･･ Notifyメッセージ受信数
other ISAKMP send packet その他のISAKMPパケット送信数
other ISAKMP receive packet
･･･････････････････････ その他のISAKMPパケット受信数

VPN discard packet･････ VPN廃棄対象パケットとして廃棄したパケット数
ESP send packet･････････ ESP送信パケット数
ESP receive packet･････ ESP受信パケット数
ESP discard packet･････ ESP廃棄パケット数
ESP replay error packet
･･･････････････････････ ESPリプレイアタックされたパケット数
ESP auth error packet･･･ ESP認証エラーパケット数
ESP send error･････････ ESP送信失敗数

13.3.2　コンソールからの操作

コンソールまたはTELNETで本装置にログインし，統計情報の表示方法を説明します．操作はノーマルモードで行います．

統計情報は，stchannel，stip，vpnstatコマンドで表示させることができます．

```
#stchannel
<private>
alignment error frames:       0
FCS error frames      :       0
collision count       :       0
<public>
alignment error frames:       0
FCS error frames      :       0
collision count       :       0
#
#
#stip
<IP>
in packet             :   338029    in discard packet       :    0
in header error packet:        0    in address error packet :    0
out request packet    :     1486    out discard packet      :    0
forward packet        :     1091    no route packet         :    2
<ICMP>
in message packet  :      122         in error packet  :      0
out message packet :      101         out error packet :      0
<UDP>
in datagram packet :   336435         in error packet    :  236737
no port packet     :        0         out datagram packet:       3
<TCP>
in segment packet :      381       out segment packet :      287
in error packet   :        0       passive open count :       61
<RIP>
in packet           :      9969     sent packet       :        2
out request packet  :         2     in reply packet   :    99669
flash update packet :         0     send error packet :        0
bad receive packet  :         0
#
#
#vpnstat
PI send packet          :        0
PI receive packet       :        0
PI discard packet       :        0
PI decrypt error packet :        0
PI hash error packet    :        0
PI exchange fail        :        0
PI exchange success     :        0
```

```
xauth send packet             :        0
xauth receive packet          :        0
xauth discard packet          :        0
xauth exchange error          :        0
xauth exchange success        :        0

PII send packet               :        0
PII receive packet            :        0
PII discard packet            :        0
PII decrypt error packet      :        0
PII hash error packet         :        0
PII exchange fail             :        0
PII exchange success          :        0

notify send packet            :        0
notify receive packet         :        0
other ISAKMP send packet      :        0
other ISAKMP receive packet   :        0

VPN discard packet            :        0
ESP send packet               :        0
ESP receive packet            :        0
ESP discard packet            :        0
ESP replay error packet       :        0
ESP auth error packet         :        0
ESP send error                :        0
```

１３．４ルーティングインタフェースの表示

ルーティングインタフェースを表示します．

１３．４．１　　Web ブラウザからの操作

Web ブラウザで，ルーティングインタフェースを表示する方法を示します．



初期画面で「インフォメーション」をクリックします．



インフォメーション画面で「ルーティングインタフェースの表示」をクリックします．



ルーティングインタフェースに関する情報が表示されます.

【項目の説明】

PRIVATE/PUBLIC ············ インタフェースの状態（up or down），RIP 送信形式，IP アドレス，サブネットマスク，ブロードキャストが表示されます.

１３.４.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，ルーティングインタフェースの表示方法を説明します．操作はノーマルモードで行います.

装置については ipinterface コマンドで表示させることができます.

```
#ipinterface
<PRIVATE>
up  broadcast
address:192.168.100.1  subnet:255.255.255.0  broadcast:192.168.100.255
<PUBLIC>
up  broadcast
```

１３.５ルーティング状態の表示

ルーティング状態の表示します.

１３.５.１　　Web ブラウザからの操作

Web ブラウザで，ルーティング状態の表示する方法を示します.



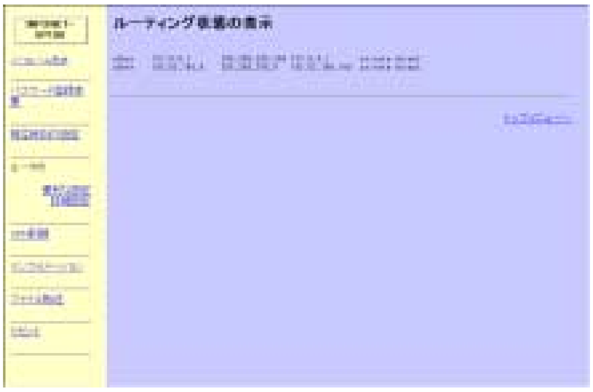
初期画面で「インフォメーション」をクリックします.

⇩



インフォメーション画面で「ルーティング状態の表示」をクリックします.

⇩



ルーティング状態が表示されます.

【項目の説明】

ルーティング情報を得た手段 （ other ， local ， rip ）

other ・・・・・・・・・・・・・・・・ 下記以外

local ・・・・・・・・・・・・・・・・ スタティック登録

rip ・・・・・・・・・・・・・・・・・・ RIP で学習

宛先 IP アドレス IP アドレスマスク

・・・・・・・・・・・・・・・・・・・・・・・・・ 宛先に到達するために送信するゲートウェイの IP アドレス

経由するインタフェース ・・・・ 経路タイプ（ direct ， indirect ）

direct ・・・・・・・・・・・・・・・ 直接ルート等の自装置内の経路を示す

indirect ・・・・・・・・・・・・・ 自装置以外の経路を示す

１３.５.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，ルーティング状態の表示方法を説明します.
操作はノーマルモードで行います.

装置については iproute コマンドで表示させることができます.

```
#iproute
rip     0.0.0.0          0.0.0.0          192.168.100.1 private indirect
other    127.0.0.1       255.255.255.255  127.0.0.1     private direct
rip     192.168.100.25   255.255.255.255  192.168.100.1 private indirect
rip     192.168.100.11   255.255.255.255  192.168.100.1 private indirect
```

１３．６ DHCP の状態表示

DHCP の状態を表示します.

１３．６．１　　Web ブラウザからの操作

Web ブラウザで，DHCP の状態を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「DHCP の状態表示」をクリックします.



DHCP の状態が表示されます．

【項目の説明】

DHCP 動作時の状態 （ a，s，S ）

a ・・・・・・・・・・・・・・・・・・・・・・ ARP の結果，存在を確認できた端末

s ・・・・・・・・・・・・・・・・・・・・・・ 動的にアドレスを割り当てた IP 端末

S ・・・・・・・・・・・・・・・・・・・・・・ 静的に割り当てている（保持している）IP 端末

MAC アドレス・・・・・・・・・・・・・・・ IP アドレスを割り当てている IP 端末の MAC アドレス

IP アドレス・・・・・・・・・・・・・・・・ IP 端末に割り当てた IP アドレス

１３.６.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，DHCP の状態の表示方法を説明します．操作はノーマルモードで行います．

DHCP の状態は，dhcpstat コマンドで表示させることができます．

```
#dhcpstat
s  xx:xx:xx:xx:xx:xx  192.168.100.10
```

１３.７ NAT+の状態表示

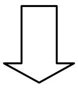
NAT+の状態を表示します.

１３.７.１　Web ブラウザからの操作

Web ブラウザで，NAT+の状態を表示する方法を示します.

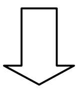


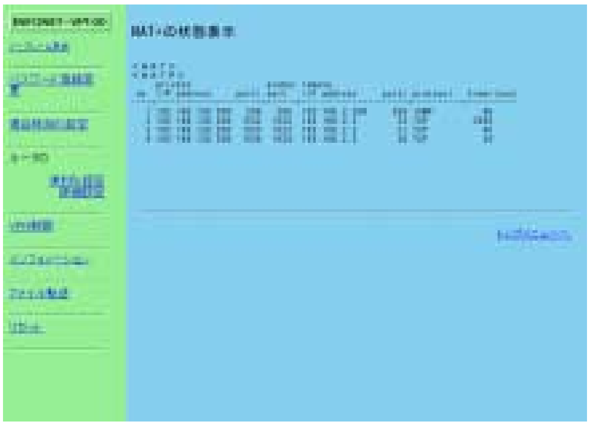
初期画面で「インフォメーション」をクリックします.





インフォメーション画面で「NAT+の状態表示」をクリックします.





NAT+の状態が表示されます.

【項目の説明】

private
- IP address ・・・・・・・・・・・・ 送信元 IP アドレス
- port ・・・・・・・・・・・・・・・・・・・ 送信元ポート番号

global port ・・・・・・・・・・・・・・ 変換後のポート番号

remote
- IP address ・・・・・・・・・・・・ 宛先 IP アドレス
- port ・・・・・・・・・・・・・・・・・・・ 宛先ポート番号

protocol ・・・・・・・・・・・・・・・・・ 変換対象のプロトコル番号

timer ・・・・・・・・・・・・・・・・・・・・ NAT 変換テーブルのエージアウトするまでの時間

１３.７.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，NAT+の状態の表示方法を説明します．操作はノーマルモードで行います．

NAT+の状態は，natinfo natp コマンドで表示させることができます．

```
#natinfo natp
    private                        global remote
 no  (IP address    port)    port  (IP address    port)   protocol  timer(sec)
----+---------------------+-------+--------------------+----------+----------
   1 192.168.138.200     256     256  192.168.2.200    256        ICMP       60
   2 192.168.138.200    1532    1532  192.168.2.2       23         TCP     3495
```

１３．８証明書表示

RSA signatures 機能で使用する証明書を表示します.

１３．８．１　Web ブラウザからの操作

Web ブラウザで，証明書を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「証明書表示」をクリックします.



証明書が表示されます.

【項目の説明】

コンソールからの操作の表示例を参照してください

１３.８.２　　コンソールからの操作

コンソールまたはTELNETで本装置にログインし，証明書の表示方法を説明します．操作はノーマルモードで行います.

証明書の表示は，vpncertinfo cert コマンドで表示させることができます.

```
#vpncertinfo cert
[1]     Subject:xxx             ←サブジェクト(証明書の所有者)
        Issuer:xxx              ←発行者
        Serial Number:xxx       ←シリアル番号
        Validity: yyyy.mm.dd hh:mm:ss - yyyy.mm.dd hh:mm:ss
                                ↑有効期間
        Domain Name:xxx         ←サブジェクトのドメイン名
        IP Address:x.x.x.x      ←サブジェクトの IP アドレス
        CRL DistPoint:xxx       ←CRL 配布点(CRL が置かれている場所)
        Key Usage:xxx           ←鍵の使用用途
```

１３．９証明書取消リスト(CRL)表示

RSA signatures 機能で使用する証明書取消リスト(CRL)を表示します.

１３．９．１　　Web ブラウザからの操作

Web ブラウザで，証明書取消リスト(CRL)を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.

⇩



インフォメーション画面で「証明書取消リスト(CRL)表示」をクリックします.

⇩



証明書取消リスト(CRL)が表示されます.

【項目の説明】

コンソールからの操作の表示例を参照してください

１３.９.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，証明書取消リスト(CRL)の表示方法を説明します．操作はノーマルモードで行います．

証明書の表示は，vpncertinfo crl コマンドで表示させることができます．

```
#vpncertinfo crl
[1]     Issuer:xxx              ←発行者
       This Update:xxx          ←更新日時
       Next Update:xxx          ←次回更新日時
```

１３.１０　　IKE SA 情報表示

IKE SA 情報を表示します.

１３.１０.１　Web ブラウザからの操作

Web ブラウザで，IKE SA 情報を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「IKE SA 情報表示」をクリックします.



IKE SA 情報が表示されます．

【項目の説明】

検索条件 ･････････････････ IKE SA 情報を ID，peer addr，peer name から検索することができます．

１３.１０.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IKE SA 情報の表示方法を説明します．操作はノーマルモードで行います．

IKE SA 情報の表示は，vpnsainfo ike コマンドで表示させることができます．

```
#vpnsainfo ike
[  1]  192.168.100.1                ←相手先アドレス
            <--> 192.168.1.1        ←自アドレス
     <R> Main Mode      UP    pre-shared key  DES   MD5
     Lifetime:1000secs              ←設定した IKE SA のライフタイム
     Current:409secs,1kbytes        ←経過時間および送信データ量
```

１３.１１　　IPSEC SA の状態表示

IPSEC SA の状態を表示します.

１３.１１.１　Web ブラウザからの操作

Web ブラウザで，IPSEC SA の状態を表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「IPSEC SA の状態表示」をクリックします.



IPSEC SA 情報が表示されます.

【項目の説明】

検索条件 ・・・・・・・・・・・・・・・・・ peer addr から検索することができます.

１３.１１.２　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IPSEC SA 情報の表示方法を説明します.操作はノーマルモードで行います.

IPSEC SA 情報の表示は，vpnsainfo ipsac コマンドで表示させることができます.

```
#vpnsainfo ipsec
1

[ 578]  192.168.100.10,255.255.255.255   ALL ALL←宛先アドレス
              <--> 192.168.200.2,255.255.255.255   ALL ALL←送信元アドレス
      peer:192.168.100.1
      <R> UP ESP DES HMAC-MD5 PFS:off
      Lifetime:                  600secs
      O-SPI:0x7fe4ffff     Current:432secs,0kbytes
       out packet      :0        error packet      :0
      I-SPI:0xc4c92fcf     Current:432secs,72kbytes
       in packet       :35       auth packet       :35
       decrypt packet  :35       discard packet    :0
       replay packet   :0        auth error packet  :0
```

【項目の説明】

peer・・・・・・・・・・・・・・・・・・・ VPN ピアアドレス

Lifetime・・・・・・・・・・・・・・・ IPsec で設定したライフタイム

O-SPI・・・・・・・・・・・・・・・・・・・ Outbound SA (自身からピア宛データ用のSA) SPI値

<Outbound>

Current・・・・・・・・・・・・・ SA確立してからの経過時間,送信データKbytes数

out packet・・・・・・・・・・ 送信パケット数

error packet・・・・・・・・ 送信エラーパケット数

I-SPI・・・・・・・・・・・・・・・・・・・ Inbounf SA (ピアから自身宛データ用のSA) SPI値

<Inbound>

Current・・・・・・・・・・・・・ SA確立してからの経過時間,受信データKbytes数

in packet・・・・・・・・・・・ 受信パケット数

auth packet・・・・・・・・・ 認証チェックしたパケット数

decrypt packet・・・・・・ 復号処理したパケット数

discard packet・・・・・・ 廃棄パケット数

replay packet・・・・・・・ リプレイアタックエラーパケット数

auth error packet・・・ 認証チェックエラーパケット数

１３.１２　　エラーログの表示

エラーログを表示します.

１３.１２.１　 Webブラウザからの操作

Webブラウザで，エラーログを表示する方法を示します.



初期画面で「インフォメーション」をクリックします.



インフォメーション画面で「エラーログの表示」をクリックします.



エラーログが表示されます.

エラーログ情報として，通し番号，装置稼働時間，日付，タスク ID，エラーコード，ログメッセージの順に表示されます.

13.12.2 コンソールからの操作

コンソールまたは TELNET で本装置にログインし，エラーログの表示方法を説明します．操作はノーマルモードで行います.

エラーログは，elog コマンドで表示させることができます.

```
#elog
seq uptime        date                        tid logid    ecode
--- ------------- ---------------------- --- -------- --------
000 0000:00:00.00 99/12/01 (wed) 16:51:31   0 00000000 00000000
                           #P_ON[V00.03-113099]
001 0000:00:00.00 99/12/06 (mon) 10:50:35   0 00000000 00000000
                           #Reset[V00.03-113099]
002 0000:00:00.00 99/12/07 (tue) 18:49:17   0 00000000 00000000
                           #Reset[V00.03-113099]
003 0000:00:00.00 99/12/09 (thu) 16:22:19   0 00000000 00000000
                           #Reset[V01.00-120399]
```

１３.１３　回線ログの表示

回線ログを表示します.

１３.１３.１　Web ブラウザからの操作

Web ブラウザで，回線ログを表示する方法を示します.



初期画面で「インフォメーション」をクリックします.

⇩



インフォメーション画面で「回線ログの表示」をクリックします.

⇩



回線ログが表示されます.

エラーログ情報として，通し番号，装置稼働時間，日付，回線種別，エラーコード，ログメッセージの順に表示されます.

13.13.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，回線ログの表示方法を説明します．操作はノーマルモードで行います.

回線ログは，llog コマンドで表示させることができます.

```
#llog
seq uptime        date                    channel  ecode
--- ------------- ----------------------- -------- --------
000 0000:00:00.00 99/12/01 (wed) 16:51:31 PRIVATE  00000000
                           #P_ON[V00.03-113099]
001 0000:00:00.00 99/12/06 (mon) 10:50:35 PRIVATE  00000000
                           #Reset[V00.03-113099]
002 0000:00:00.00 99/12/07 (tue) 18:49:17 PRIVATE  00000000
                           #Reset[V00.03-113099]
000 0000:00:00.00 99/12/01 (wed) 16:51:31 PUBLIC   00000000
                           #P_ON[V00.03-113099]
001 0000:00:03.78 99/12/01 (wed) 16:51:35 PUBLIC   08050200
                           Ethernet Tx error
002 0000:00:00.00 99/12/06 (mon) 10:50:35 PUBLIC   00000000
                           #Reset[V00.03-113099]
```

１３.１４　　イベントログの表示

イベントログを表示します.

１３.１４.１　Web ブラウザからの操作

Web ブラウザで，イベントログを表示する方法を示します.



初期画面で「インフォメーション」をクリックします.

⇩



インフォメーション画面で「イベントログの表示」をクリックします.

⇩



イベントログが表示されます．

イベントログ情報として，通し番号，装置稼働時間，日付，タスク ID，ログ ID，エラーコード，ログメッセージの順に表示されます．

13.14.2 コンソールからの操作

コンソールまたは TELNET で本装置にログインし，イベントログの表示方法を説明します．操作はノーマルモードで行います．

イベントログは，vlog コマンドで表示させることができます．

```
#vlog
seq uptime        date                     tid  logid    ecode
--- ------------- ----------------------- --- -------- --------
000 0000:00:00.00 99/12/22 (wed) 10:10:32   0 00000000 00000000
                             #P_ON[V01.02-122199]
001 0000:00:00.00 99/12/22 (wed) 22:15:38   0 00000000 00000000
                             #Reset[V01.02-122199]
002 0000:35:51.60 99/12/22 (wed) 22:51:29  10 00000000 00000000
                             telnet login fail from 192.168.138.200
003 0000:36:01.60 99/12/22 (wed) 22:51:39  10 00000000 00000000
                             telnet login success from 192.168.138.200
```

１３.１５　　VPN ログの表示

VPN ログを表示します.

１３.１５.１　Web ブラウザからの操作

Web ブラウザで，VPN ログを表示する方法を示します.



初期画面で「インフォメーション」をクリックします.

⇩



インフォメーション画面で「VPN ログの表示」をクリックします.

⇩



VPN ログが表示されます.

VPN ログ情報として，通し番号，装置稼働時間，日付，タスク ID，ログ ID，エラーコード，ログメッセージの順に表示されます.

13.15.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，VPN ログの表示方法を説明します．操作はノーマルモードで行います.

VPN ログは，vpnlog コマンドで表示させることができます.

```
#vpnlog
seq uptime        date                    tid logid    ecode
--- ------------- ----------------------- --- -------- --------
000 0009:35:46.66 99/12/23 (thu) 07:51:24  27 1b000321 00000000
                           #P_ON[V00.03-113099]
001 0009:35:47.33 99/12/23 (thu) 07:51:25  27 1b000221 00000000
                           IPSEC SA is created. 192.168.150.1
002 0009:44:17.13 99/12/23 (thu) 07:59:55  27 1b000221 00000000
                           IPSEC SA is created. 192.168.150.1
003 0009:52:49.37 99/12/23 (thu) 08:08:27  27 1b000321 00000000
                           IKE SA is created. 192.168.150.1
004 0009:52:50.06 99/12/23 (thu) 08:08:28  27 1b000221 00000000
                           IPSEC SA is created. 192.168.150.1
```

１３.１６　　通信パケットログの表示

通信パケットログを表示します．ログに掲載する通信パケットは，「通信パケットログの設定（P１２-3）」で設定します．

１３.１６.１　Web ブラウザからの操作

Web ブラウザで，通信パケットログを表示する方法を示します．



初期画面で「インフォメーション」をクリックします．

⇩



インフォメーション画面で「通信パケットログの表示」をクリックします．

⇩



通信パケットログが表示されます.

通信パケットログ情報として，通し番号，日付，通信パケットの情報の順に表示されます.

13.16.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，通信パケットログの表示方法を説明します.
操作はノーマルモードで行います.

通信パケットログは，clog コマンドで表示させることができます.

```
#clog
seq date
--- -----------------------
000 00/08/18 (fri) 16:23:54
    #Reset [V03.00-080700]
001 00/08/18 (fri) 16:24:37
    RECV public,
    TCP(S):158.202.234.171:1494->158.202.232.6:80
```

１３.１７　　IP パケットフィルター廃棄ログの表示

IP パケットフィルター廃棄ログを表示します．IP パケットフィルター廃棄ログを表示するかどうかは，「IP パケットフィルター廃棄ログの設定（P１２-4）」で設定します．

１３.１７.１　Web ブラウザからの操作

Web ブラウザで，IP パケットフィルター廃棄ログを表示する方法を示します．



初期画面で「インフォメーション」をクリックします．

⇩



インフォメーション画面で「IP パケットフィルター廃棄ログの表示」をクリックします．

⇩



IP パケットフィルター廃棄ログが表示されます.

IP パケットフィルター廃棄ログ情報として，通し番号，日付，IP パケットフィルター廃棄ログの情報の順に表示されます.

13.17.2 コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IP パケットフィルター廃棄ログの表示方法を説明します．操作はノーマルモードで行います.

IP パケットフィルター廃棄ログは，flog コマンドで表示させることができます.

```
#flog
seq date
--- -----------------------
000 00/08/18 (fri) 16:23:54
    #Reset [V03.00-080700]
001 00/08/18 (fri) 16:24:37
    RECV recv from public,
    ICMP:192.168.100.1->192.52.150.100, type 8, code 0
```

１３.１８　　IP パケットフィルター廃棄ログの表示

IP パケットフィルター廃棄ログを表示します．IP パケットフィルター廃棄ログを表示するかどうかは，「IP パケットフィルター廃棄ログの設定（P１２-4）」で設定します．

１３.１８.１　　Web ブラウザからの操作

Web ブラウザで，IP パケットフィルター廃棄ログを表示する方法を示します．



初期画面で「インフォメーション」をクリックします．



インフォメーション画面で「IP パケットフィルター廃棄ログの表示」をクリックします．



IP パケットフィルター廃棄ログが表示されます.

IP パケットフィルター廃棄ログ情報として，通し番号，日付，IP パケットフィルター廃棄ログの情報の順に表示されます.

13.18.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IP パケットフィルター廃棄ログの表示方法を説明します．操作はノーマルモードで行います.

IP パケットフィルター廃棄ログは，flog コマンドで表示させることができます.

```
#flog
seq date
--- -----------------------
000 00/08/18 (fri) 16:23:54
    #Reset [V03.00-080700]
001 00/08/18 (fri) 16:24:37
    RECV recv from public,
    ICMP:192.168.100.1->192.52.150.100, type 8, code 0
```

１３.１９　　ルータグループの表示

ルータグループ機能使用時の，装置の状態を表示します．

１３.１９.１　Web ブラウザからの操作

Web ブラウザで，IP パケットフィルター廃棄ログを表示する方法を示します．



初期画面で「インフォメーション」をクリックします．



インフォメーション画面で「ルータグループの状態表示」をクリックします．



ルータグループの情報が表示されます.

IP パケットフィルター廃棄ログ情報として，通し番号，日付，IP パケットフィルター廃棄ログの情報の順に表示されます.

13.19.2　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IP パケットフィルター廃棄ログの表示方法を説明します．操作はノーマルモードで行います.

IP パケットフィルター廃棄ログは，flog コマンドで表示させることができます.

```
#flog
seq date
--- -----------------------
000 00/08/18 (fri) 16:23:54
    #Reset [V03.00-080700]
001 00/08/18 (fri) 16:24:37
    RECV recv from public,
    ICMP:192.168.100.1->192.52.150.100, type 8, code 0
```

14オペレーション

WEB設定または，コマンドラインから各種オペレーションがおこなえます.
操作できる項目は以下の通りです.

VPN制御

ファイル転送

リセット

以下項目は，コマンドラインのみです.

ping

フレームトレース

１４．１VPN 制御について

VPN 制御について説明します．

VPN 制御には，IKE SA 解放と IPSEC SA 解放，証明書リクエスト生成，CRL 取得があります．

証明書リクエスト生成については，６-11をご覧下さい．

１４．２IKE SA／IPSEC SA 開放

指定した IKE または IPSEC SA を開放します．

１４．２．１　　Web ブラウザからの操作

Web ブラウザで，IKE または IPSEC SA の開放を行う方法を示します．



初期画面で「VPN 制御」をクリックします．

⇩



VPN 制御画面で「IKE SA 解放」をクリックします．

※「IKE SA 解放」を例に説明しますが，「IPSEC SA 解放」も操作は同じです．

⇩



IKE SA 解放画面で，解放条件を選択した後に「送信」をクリックします．

【項目の説明】
全ての IKE SA を解放する・・・ 全ての IKE SA を解放します．

SAID を指定して IKE SA を解放する SAID
・・・・・・・・・・・・・・・・・・・・・・・・・ SAID を指定して IKE SA を解放します．

１４.２.２　　コンソールからの操作

コンソールまたは TELNET で本装置にログインし，IKE SA/IPSEC SA を開放する方法を説明します．操作はノーマルモードで行います．
IKE SA 解放，IPSEC SA 解放については ikeclear，ipsecclear コマンドを使用します．

ｉｋｅｃｌｅａｒ{<said>|all}
ｉｐｓｅｃｃｌｅａｒ{<said>|all}

パラメータ
said・・・・・・・・・・・・・・・・・・・・ SAID を指定して IKE SA を解放します．

all・・・・・・・・・・・・・・・・・・・・・ 全ての IKE SA を解放するします．

１４．３ CRL 取得

CRL（Certificate Revocation List：証明書取り消しリスト）を取得します．CRL は，通常次のアップデート日時が決まっているため，CRL を使用する時にアップデート日時が過ぎていたら自動で新しい CRL を取得しますが，この操作では手動で CRL を取得することができます．

１４．３．１　　Web ブラウザからの操作

Web ブラウザで，CRL 取得を行う方法を示します．



初期画面で「VPN 制御」をクリックします．

⇩



VPN 制御画面で「CRL 取得」をクリックします．

⇩



取得するCRLのURLを選択し，「取得」をクリックします.

１４.３.２　　コンソールからの操作

コンソールまたはTELNETで本装置にログインし，CRL取得方法を説明します．操作はノーマルモードで行います.

CRLの取得は，vpncrlgetコマンドを使用します.

```
#vpncrlget
[1]   :http://xxx.xxx.com/crls/ca1.crl
Select no : 1
ok
```

１４.４ファイル転送について

ファイル転送について説明します.

VPN 制御には，「ファームウエアをアップデートする」，「ルータ設定ファイルをアップデートする」，「ルータ設定ファイルをダウンロードする」があります.

１４.４.１　　Web ブラウザからの操作（ファームウエアをアップデートする）

Web ブラウザで，ファームウエアをアップデートする方法を示します.



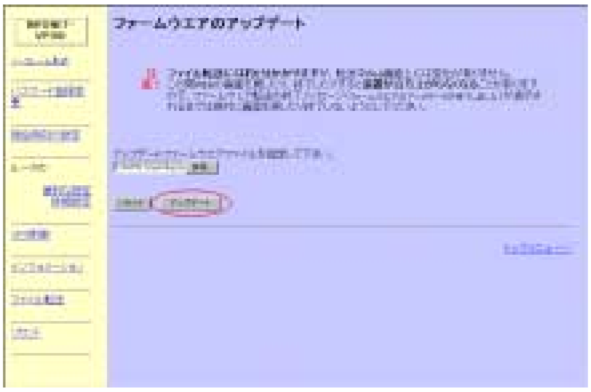
初期画面で「ファイル転送」をクリックします.

⇩



ファイル転送画面で「ファームウェアのアップデート」をクリックします.

⇩



ファームウェアのアップデート画面で，アップデートファームウエアファイルを入力または参照した後にアップデートボタンをクリックします.

１４.４.２　　Web ブラウザからの操作（ルータ設定ファイルをアップデートする）

Web ブラウザで，ルータ設定ファイルをアップデートする方法を示します.



初期画面で「ファイル転送」をクリックします.



ファイル転送画面で「ルータ設定ファイルをアップデートする」をクリックします.



ルータ設定ファイルのアップデート画面で，アップデートを行うルータ設定ファイルを入力または参照した後にアップデートボタンをクリックします.

１４.４.３　　Web ブラウザからの操作（ルータ設定ファイルをダウンロードする）

Web ブラウザで，ルータ設定ファイルをダウンロードする方法を示します.



初期画面で「ファイル転送」をクリックします.



ファイル転送画面で「ルータ設定ファイルをダウンロードする」をクリックします.



ルータ設定ファイルのダウンロード画面で，ダウンロードボタンをクリックします.
ダウンロードボタンを押した後に，ファイルの保存先を指定します.

１４.５ｐｉｎｇ

ping について説明します.

コンソールまたは TELNET で本装置にログインし，ping の使用方法を説明します．操作はノーマルモードで行います.

ping コマンドを使うことにより，IP 接続の確認を行えます.

ｐｉｎｇ<IP address>

パラメータ

IP address･･････････････ 接続確認を行いたい端末の IP アドレスを入力します.

画面例を以下に示します.

```
#ping 192.168.100.1
64 bytes from 192.168.100.1: icmp_seq=0.

---- PING Statistics ----
1 packets transmitted, 1 packets received,
```

１４.６トレースルートについて

トレースルートについて説明します．

コンソールまたは TELNET で本装置にログインし，トレースルートの使用方法を説明します．操作はノーマルモードで行います．

traceroute コマンドを使うことにより，目的の宛先までの経路（ルータ）を調べます

ｔｒａｃｅｒｏｕｔｅ [-m <max_ttl>] [-p <port#>] <IP address>

オプション

-m<max_ttl>･･････････････ 最大検索経路数の指定．検索する経路数を指定します．指定の経路数以上の調査は行いません．
デフォルトは 32 です．

-p <port#>･･････････････ ポート番号の指定．経路数を調べるときに使用するポート番号を指定します．
デフォルトは 33434 です．

パラメータ

IP address･･････････････ 調べる先の IP アドレス

画面例を以下に示します．

```
#traceroute 192.168.224.2

  1 192.168.232.6  14 ms  7 ms  13 ms
  2 192.168.50.1  2 ms  18 ms  2 ms
  3 192.168.48.127  5 ms  4 ms  25 ms
  4 192.168.160.254  219 ms  260 ms  218 ms
  5 192.168.224.2  348 ms  224 ms  291 ms
```

INFONET-VP100 VPN ボックス

取扱説明書４版

発行日　２０００年　９月

発行責任　古河電気工業株式会社

Printed in Japan

- 本書は改善のため事前連絡なしに変更することがあります.
- 本書に記載されたデータの使用に起因する第三者の特許権その他の権利については,当社はその責を負いません.
- 無断転載を禁じます.
- 落丁・乱丁本はお取り替えいたします.